

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМ. П. Г. ДЕМИДОВА

В. Н. Князев, Д. М. Мурин

**БЕЗОПАСНОСТЬ**  
**В СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ СРЕДЕ**  
**Часть 1**

*Учебное пособие*

Ярославль 2021

УДК 004.056  
ББК 32.972.53я73  
К54

Рецензенты:

Кафедра высшей математики РГТУ им. П. А. Соловьева;  
Старший преподаватель кафедры социального и семейного законодательства  
ЯрГУ им. П. Г. Демидова, кандидат юридических наук С. В. Симонова

**Князев, Владимир Николаевич.**  
**Безопасность в современной информационной**  
**среде. Часть 1:** учебное пособие / В. Н. Князев,  
К 54 Д. М. Мурин; Яросл. гос. ун-т им. П. Г. Демидова. —  
Ярославль: ИНДИГО, 2021. – 158 с.

ISBN 978-5-91722-426-8

В первой части пособия рассмотрены правовые и организационные основы обеспечения информационной безопасности в Российской Федерации, а также основы информационной безопасности в операционных системах. В качестве основного объекта защиты рассматриваются персональные данные, но рассматриваемые подходы справедливы и при защите других видов конфиденциальной информации. Существенное внимание уделено описанию процесса обеспечения безопасности информации и обзору современных видов средств защиты информации.

Предназначено для бакалавров нетехнических специальностей и направлений подготовки.

Пособие подготовлено с использованием издательской системы L<sup>A</sup>T<sub>E</sub>X.

Табл. 4. Рис. 38. Библиогр.: 28 назв.

УДК 004.056  
ББК 32.972.53я73

ISBN 978-5-91722-426-8

© ЯрГУ, 2021

# Оглавление

<b>Список основных обозначений и аббревиатур</b>	<b>7</b>
<b>Введение</b>	<b>9</b>
<b>1. Правовые основы обеспечения информационной безопасности</b>	<b>11</b>
1.1. Основные права граждан в сфере обработки и защиты информации . . . .	11
1.2. Информация и ее свойства . . . . .	12
1.3. Классификация информации по возможности доступа и с точки зрения возможности распространения . . . . .	15
1.4. Информационные технологии и информационные системы . . . . .	18
1.5. Ответственность в сфере обработки и защиты конфиденциальной информации . . . . .	22
1.6. Вопросы и задания . . . . .	27
<b>2. Защита персональных данных</b>	<b>28</b>
2.1. Правовые акты в области обработки и защиты персональных данных . . .	28
2.2. Обработка персональных данных. Основные понятия и их определения . .	32
2.3. Принципы обработки персональных данных . . . . .	34
2.4. Основания обработки персональных данных . . . . .	36
2.5. Согласие субъекта на обработку его персональных данных . . . . .	37
2.6. Поручение обработки персональных данных . . . . .	39
2.7. Трансграничная передача персональных данных . . . . .	40
2.8. Особые категории персональных данных . . . . .	41
2.8.1. Общедоступные источники персональных данных и персональные данные, разрешенные для распространения . . . . .	41
2.8.2. Специальные категории персональных данных . . . . .	42
2.8.3. Биометрические персональные данные . . . . .	44
2.9. Права субъекта персональных данных . . . . .	45
2.10. Меры обеспечения безопасности персональных данных . . . . .	48
2.11. Контроль и надзор за выполнением мер по обеспечению безопасности . . .	50
2.12. Вопросы и задания . . . . .	51
<b>3. Организационные основы обеспечения информационной безопасности</b>	<b>53</b>
3.1. Организационные основы обеспечения информационной безопасности. Алгоритм действий . . . . .	53
3.2. Выявление и анализ информационных активов . . . . .	57
3.3. Моделирование нарушителей и угроз информационной безопасности . . . .	59
3.3.1. Моделирование нарушителей . . . . .	60
3.3.2. Моделирование угроз информационной безопасности . . . . .	63
3.4. Категорирование, классификация, определение уровней защищенности . .	64
3.5. Проектирование системы защиты информации . . . . .	66
3.5.1. Типовые проектные решения для систем защиты информации . . . .	73
3.6. Разработка организационной и эксплуатационной документации . . . . .	75
3.7. Внедрение системы защиты информации . . . . .	75
3.8. Оценка соответствия объекта информатизации . . . . .	76
3.9. Эксплуатация . . . . .	78
3.10. Лицензирование . . . . .	78
3.11. Вопросы и задания . . . . .	79

<b>4. Архитектура компьютера</b>	<b>81</b>
4.1. Процессоры . . . . .	81
4.1.1. Интерпретация . . . . .	82
4.1.2. Системы RISC и CISC . . . . .	83
4.1.3. Как можно сделать процессор более производительным? . . . . .	84
4.1.4. Мультипроцессоры (многоядерные процессоры) . . . . .	84
4.1.5. SIMD-процессоры . . . . .	85
4.2. Память . . . . .	86
4.2.1. Иерархическая структура памяти . . . . .	87
4.2.2. Регистры процессора . . . . .	88
4.2.3. Кэш-память . . . . .	89
4.2.4. Основная (оперативная) память . . . . .	90
4.2.5. Жесткие магнитные диски . . . . .	91
4.2.6. Твердотельные накопители . . . . .	93
4.3. Устройства ввода-вывода . . . . .	94
4.3.1. Шины . . . . .	94
4.3.2. Клавиатуры . . . . .	97
4.3.3. Мыши . . . . .	97
4.3.4. Плоские мониторы . . . . .	98
4.3.5. Сенсорные экраны . . . . .	99
4.3.6. Принтеры . . . . .	101
4.3.7. Веб-камеры . . . . .	102
4.3.8. Микрофоны . . . . .	103
4.3.9. Динамические (катушечные) микрофоны . . . . .	103
4.3.10. Конденсаторные микрофоны . . . . .	104
4.4. Вопросы и задания . . . . .	105
<b>5. Основы операционных систем</b>	<b>107</b>
5.1. Введение . . . . .	107
5.2. Определение операционной системы . . . . .	107
5.2.1. ОС как провайдер ресурсов . . . . .	108
5.2.2. ОС как менеджер ресурсов . . . . .	110
5.3. Основные понятия операционной системы . . . . .	112
5.3.1. Режим ядра и режим пользователя . . . . .	112
5.3.2. Прерывания . . . . .	113
5.3.3. Системные вызовы . . . . .	114
5.3.4. Приложения, процессы, потоки . . . . .	114
5.3.5. Планировщик и смена контекста . . . . .	117
5.3.6. Управление памятью . . . . .	119
5.3.7. Файловые системы . . . . .	121
5.4. Безопасность операционной системы . . . . .	123
5.4.1. Управление доступом . . . . .	123
5.4.2. Дискреционное управление доступом . . . . .	124
5.4.3. Ролевое разграничение доступа . . . . .	124
5.4.4. Мандатное управление доступом . . . . .	125
5.4.5. Модель целостности Биба . . . . .	126
5.4.6. Привилегии . . . . .	127
5.4.7. Идентификация . . . . .	127

5.4.8. Аутентификация . . . . .	127
5.4.9. Авторизация . . . . .	129
5.5. Вопросы и задания . . . . .	130
<b>6. Безопасность ОС Windows</b>	<b>133</b>
6.1. Субъекты доступа . . . . .	133
6.1.1. Токен доступа . . . . .	133
6.1.2. Идентификаторы . . . . .	134
6.1.3. Уровни целостности . . . . .	134
6.1.4. Привилегии . . . . .	135
6.2. Объекты доступа . . . . .	136
6.2.1. Дескриптор безопасности . . . . .	136
6.2.2. Дискреционные списки управления доступом . . . . .	136
6.2.3. Уровни целостности . . . . .	139
6.3. Права владельца . . . . .	139
6.4. Алгоритм определения правомерности доступа . . . . .	139
6.5. Аудит . . . . .	140
6.6. Аутентификация . . . . .	141
6.7. Вопросы и задания . . . . .	141
<b>7. Безопасность ОС Linux</b>	<b>144</b>
7.1. Субъекты доступа . . . . .	144
7.1.1. Пользователи . . . . .	144
7.1.2. Группы . . . . .	145
7.1.3. Привилегированные программы: биты установки UID и GID . . . . .	145
7.1.4. Привилегии . . . . .	146
7.2. Объекты доступа . . . . .	148
7.2.1. Права . . . . .	149
7.2.2. Биты SUID, SGID и Sticky . . . . .	150
7.2.3. Списки управления доступом . . . . .	150
7.3. Авторизация . . . . .	151
7.3.1. Базовый алгоритм определения правомерности доступа . . . . .	151
7.3.2. Алгоритм определения правомерности доступа для файлов со списком доступа . . . . .	152
7.4. Аутентификация . . . . .	152
7.5. Вопросы и задания . . . . .	153
<b>Список использованной литературы</b>	<b>155</b>



## Список основных обозначений и аббревиатур

АЛУ	арифметико-логическое устройство;
АРМ	автоматизированное рабочее место (ПЭВМ и вспомогательные технические средства);
МОПЗ	блок операций с плавающей запятой;
ГИБДД	Государственная инспекция безопасности дорожного движения;
ДСУД	дискреционный список управления доступом;
ЖК	жидкокристаллический;
ИС	информационная система;
ИСПДн	информационная система персональных данных;
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях;
ОС	операционная система;
ПАО	публичное акционерное общество;
ПЗС	прибор с зарядовой связью;
ПК	персональный компьютер;
ПДн	персональные данные;
ПО	программное обеспечение;
РФ	Российская Федерация;
ССУД	системный список управления доступом;
УЗ	уровень защищенность;
УК РФ	Уголовный кодекс Российской Федерации;
ФЗ	федеральный закон;
ФС	файловая система;
ФСБ России	Федеральная служба безопасности Российской Федерации;
ФСТЭК России	Федеральная служба технического и экспортного контроля Российской Федерации;
ЦАФАП	Центр автоматизированной фиксации административных правонарушений в области дорожного движения;
ЦОД	центр обработки данных;
CISC	компьютер с набором сложных команд;
CRM	система управления взаимоотношениями с клиентами;
DRAM	динамическая память с произвольным доступом;
ERP	система управления предприятием;
EGID	эффективный (текущий) GID;
EUID	эффективный (текущий) UID;

GPU	графический процессор;
GID	идентификатор группы по умолчанию пользователя, запустившего поток;
HAL	уровень абстракции оборудования;
HDD	жесткий магнитный диск;
IDE/ATA	параллельный интерфейс обмена данными;
ISA	промышленный стандарт шинной архитектуры;
MIMD	(концепция) множественный поток команд, множественный поток данных;
RAM	память с произвольным доступом;
RISC	компьютер с сокращенным набором команд;
PCI	(стандарт) подключения периферийных компонентов;
SATA	последовательный интерфейс обмена данными;
SID	идентификатор безопасности;
SIEM	систем менеджмента информационной безопасности и управления событиями безопасности;
SIMD	(концепция) одиночный поток команд, множественный поток данных;
SSD	твердотельный накопитель;
UID	идентификатор пользователя, запустившего поток.



# Введение

Основной целью курса «Безопасность в современной информационной среде» является подготовка бакалавров нетехнических специальностей и направлений подготовки к деятельности, связанной с использованием современных средств и методов защиты информации в повседневной и профессиональной деятельности.

При разработке курса мы исходим из необходимости повышения общего уровня осведомленности граждан Российской Федерации в области информационной безопасности. Всеобщее обучение информационной безопасности должно стать основой для формирования коллективной (общественной) информационной безопасности, понимаемой как согласованность (общность) оценок и действий различных членов общества при реакции на существующие и возникающие угрозы информационной безопасности.

В пособии мы осознанно опускаем некоторые технические детали, акцентируя внимание на принципиальных идеях и подходах к обеспечению информационной безопасности. В качестве основного объекта защиты мы рассматриваем конфиденциальную информацию, в том числе персональные данные.

В первой части пособия рассмотрены правовые и организационные основы обеспечения информационной безопасности в Российской Федерации, а также штатные средства обеспечения информационной безопасности в операционных системах.

Первая глава посвящена правовым основам обеспечения информационной безопасности. В ней мы изучим основные конституционные права граждан Российской Федерации в области обработки и защиты информации; познакомимся с положениями федерального закона, регулирующего сферу обработки информации, информатизации и защиты информации; изучим основные свойства безопасности информации: конфиденциальность, целостность, доступность, а также познакомимся с различными видами тайн; приведем классификации информации по возможностям доступа и распространения. Кроме того, мы рассмотрим различные виды информационных систем и узнаем права и обязанности обладателя информации и оператора информационной системы, а в заключение обсудим вопрос ответственности в сфере обработки и защиты информации.

Во второй главе рассматриваются вопросы защиты персональных данных. В ней мы познакомимся с различными видами персональных данных и изучим принципы и условия их обработки; узнаем, какими правами обладают субъекты персональных данных и по каким причинам они могут быть ограничены; изучим права и обязанности оператора (персональных данных). Также в этой главе мы рассмотрим меры обеспечения безопасности персональных данных и узнаем, какие государственные органы осуществляют контроль и надзор в сфере обработки и защиты персональных данных.

В третьей главе мы рассмотрим общий порядок обеспечения информационной безопасности. В качестве этапов процесса обеспечения информационной безопасности мы выделяем: этап выявления и анализа информационных активов; этап формирования требований по защите информации, включающий моделирование нарушителей и угроз информационной безопасности; этап выбора средств и методов защиты информации; этап внедрения системы защиты информации и этап эксплуатации системы защиты информации. Мы описываем подходы, которые можно использовать при реализации каждого этапа, а также планируемые результаты, которые должны быть достигнуты по итогам каждого этапа.

В четвертой главе познакомимся с архитектурой компьютера, что необходимо для дальнейшего изучения курса. Мы узнаем принципы работы основных элементов компьютера: процессора, оперативной и вспомогательной памяти, устройств ввода-вывода (шины, монитора, клавиатуры и мыши, веб-камеры, принтеров и динамических и конденсаторных микрофонов), а также познакомимся с такими понятиями, как «интерпретация» и «иерархическое устройство памяти».

Пятая глава посвящена введению в информационную безопасность операционных систем. В начале главы рассматриваются общие методы хранения и обработки информации на компьютере, даются определения понятиям «операционная система» и «файловая система». Затем изучаются методы управления доступом в информационных (компьютерных) системах: дискреционное управление доступом, мандатное управление доступом и ролевое управление доступом. Кроме того, рассматриваются подходы к идентификации, аутентификации и авторизации пользователей компьютерных систем, в том числе аутентификация на основе паролей, на основе внешних носителей ключа и биометрическая аутентификация.

Шестая глава посвящена особенностям управления доступа в операционных системах семейства Windows, а седьмая — в операционных системах семейства Linux. Рассматриваются подходы к идентификации, аутентификации и авторизации пользователей в таких системах, а также к реализации процесса аудита.

При подготовке первой части пособия использовались источники, приведенные в списке литературы. При освещении правовых вопросов мы старались придерживаться действующих положений нормативных, правовых и методических документов, регулирующих вопросы обработки и защиты информации. При этом мы приводим большое число примеров применения этих положений, а также возможные трактовки дискуссионных положений. Существенную роль при подготовке технических глав пособия сыграли книги Эндрю Таненбаума, которые мы рекомендуем для более углубленного изучения материала.

Все рисунки, используемые в пособии, отрисованы авторами самостоятельно. Сторонние изображения не использовались в качестве исходного материала для создания рисунков в пособии, за исключением сложных технических средств (жесткого диска, монитора, клавиатуры и т. п.), исходные изображения которых получены с сайта <https://pixabay.com/> и, возможно, изменены и дополнены. Рисунок 9 основан на рисунке [28], который является общественным достоянием. Рисунок 12 основан на рисунке из работы [20]. Возможная схожесть с рисунками других авторов объясняется иллюстрацией аналогичных идеи и концепции.

# 1. Правовые основы обеспечения информационной безопасности

## 1.1. Основные права граждан в сфере обработки и защиты информации

Основные права и свободы граждан Российской Федерации закреплены в Конституции нашей страны. В том числе в ней содержатся базовые положения, касающиеся вопросов обработки и защиты информации. Так, часть 4 статьи 29 Конституции Российской Федерации устанавливает, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым **законным** способом.

Обратим внимание, что такая формулировка неявно содержит определенную проблему. Раскрывая приведенное ранее положение Конституции Российской Федерации на практическом уровне, мы сталкиваемся с необходимостью описания либо всех законных, либо всех «незаконных» способов «обработки» информации. С технической точки зрения реализуемы (и получили широкое распространение) оба подхода. Первый из них получил название «запрещено все, что не разрешено», второй — «разрешено все, что не запрещено». С юридической же точки зрения существенным преимуществом пользуется второй подход, что приводит к определенному состязанию. Зная описание «незаконных» способов обработки информации (ввиду общедоступности правовых актов), «злоумышленник» получает возможность искать способы достижения своих целей, не попадающие под известные ему описания.

Обеспечение безопасности информации при этом во многом состоит в создании таких условий, при которых злоумышленник будет вынужден добиваться своих целей, используя явно описанные «незаконные» способы обработки информации.

Руководствуясь принципом, что свобода одного человека заканчивается там, где начинается свобода другого, мы можем понимать защиту информации как создание определенных «барьеров», столкновение с которыми должно явно свидетельствовать, что реализация желаемых действий, включающая преодоление таких «барьеров», ведет к нарушению закона.

В уже упомянутой нами статье 29 Конституции Российской Федерации также упоминается первый встретившийся нам вид защищаемой информации — государственная тайна. Исторически это самый древний и во многом самый защищаемый вид информации.

Кроме государственной тайны, в статьях 23 и 24 Конституции Российской Федерации фактически приводится второй вид защищаемой информации — персональные данные. Так, в статье 23 устанавливается, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, а в статье 24 отмечается, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Отметим также, что согласно статье 71 Конституции Российской Федерации (пункты и, м) информация, информационные технологии и связь, а также обеспечение безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных относятся к ведению Российской Федерации.

Положения Конституции Российской Федерации конкретизируются в федеральных законах (включая кодексы), в указах Президента Российской Федерации и

постановлениях Правительства Российской Федерации, а также в ведомственных правовых и методических документах.

Основным федеральным законом, регулирующим сферу обработки информации, является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Указанный федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

С точки зрения защиты информации, основными принципами правового регулирования, установленными рассматриваемым законом, являются:

1. Свобода поиска, получения, передачи, производства и распространения информации любым **законным** способом.
2. Обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации.
3. Установление ограничений доступа к информации только федеральными законами.
4. Достоверность информации и своевременность ее предоставления.
5. Неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Федеральный закон «Об информации, информационных технологиях и о защите информации» вводит определения базовых понятий в сфере обработки и защиты информации, которые используются во всем правовом поле Российской Федерации.

## 1.2. Информация и ее свойства

Очевидно, что основным понятием в рассматриваемой сфере является понятие «Информация». Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»:

**Определение 1.1.** ***Информация** — это сведения (сообщения, данные) независимо от формы их представления.*

Обратим внимание, что это определение является очень общим. Оно не требует, чтобы сведения были каким-либо образом структурированы, были зафиксированы на каком-либо носителе и т. п.

Следует особо подчеркнуть независимость сведений от формы представления. Говоря о формах представления информации, мы обычно понимаем, что информация может быть записана от руки на листочке (например, имя, адрес и телефон нового знакомого), напечатана на бумажном носителе (например, в книгах, брошюрах, на листовках,

плакатах), представлена в виде файлов различных форматов в наших компьютерах, планшетах, смартфонах и т. п.

Кроме того, информацией можно обмениваться. Мы общаемся друг с другом, говорим и слышим, показываем и видим, пишем электронные сообщения и прикладываем к ним фотографии, читаем эти сообщения. Во всех этих процессах информация передается по «каналам связи» и может быть представлена в виде акустических, оптических, радио- или электромагнитных сигналов.

Если еще немного углубиться, то говоря, что «файлы с информацией обрабатываются на компьютере», мы понимаем компьютер как законченное целое. На самом деле он является сложной системой, состоящей из множества различных элементов, некоторые из которых могут выступать как «приемниками», так и «передатчиками» информации. Кроме того, для взаимодействия между элементами компьютера существуют особые «каналы связи» (например, шины) внутри компьютера.

Таким образом, «файлы с информацией, обрабатываемые на компьютере», на самом деле могут храниться на жестком диске в форме особым образом намагниченной области, могут находиться в оперативной памяти, передаваться по каналам материнской платы и обрабатываться процессором в виде электромагнитных сигналов. Более того, в процессе обработки информации различные элементы компьютера формируют электромагнитные поля, которые также будут являться носителями (обрабатываемой) информации.

Отметим, что, с точки зрения данного выше определения понятия «информация», наши мысли также являются информацией. При этом, с одной стороны, человек как носитель мыслей может рассматриваться в качестве объекта защиты. С другой стороны, нарушитель, не обладая техническими средствами, может подсмотреть информацию или подслушать. Поскольку защита человека реализуется скорее в правовом, организационном и физическом смысле, а наше пособие в большей степени ориентировано на вопросы технической защиты информации, то мы скорее рассматриваем человека как нарушителя, а не объект защиты.

При работе с информацией мы предъявляем к ней определенные требования. Например, мы можем предъявлять требования к форме ее представления, объему данных, новизне и так далее. С точки зрения информационной безопасности выделяются три основных свойства безопасности информации («три кита»): **конфиденциальность, целостность и доступность**.

**Определение 1.2.** *Конфиденциальность информации — это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.*

Другими словами, конфиденциальность понимается как некоторое ограничение, наложенное на информацию ее владельцем. Каждый, кто желает получить такую информацию, должен согласиться с тем условием, что он не может своим собственным решением передать такую (конфиденциальную) информацию третьим лицам, а должен предварительно получить согласие обладателя на передачу или обеспечить получение третьей стороной информации непосредственно у обладателя.

Согласитесь, что если мы доверяем кому-то напечатать наши фотографии, то мы (по крайней мере в некоторых случаях) хотим быть уверенными в том, что завтра не найдем эти фотографии в сети Интернет. Или вряд ли мы будем рады, если обнаружим в сети Интернет данные своей банковской карты или копию медицинской книжки.

Не менее значимой характеристикой информации является **целостность**. Каждый из нас, положив в карман 1000 рублей, надеется их там обнаружить. В данном

случае информация, которой являются сведения о номинале купюры, неразрывно связана с физическим носителем — то есть собственно купюрой. Ситуация существенно усложняется, если связь информации с «носителем» утрачивается или полностью исчезает.

Например, мы положили на банковский счет 100.000 рублей (будем считать, что процентная ставка не отрицательная) и не предпринимали никаких действий по снятию средств. Согласитесь, что все мы надеемся через какое-то время обнаружить на счету как минимум 100.000 и 10.000 нас явно расстроят. При этом доступные нам на банковском счете средства представляют собой записи в некоторой базе данных, значения которых можно изменять. Естественно, к данным нашего банковского счета можем иметь доступ не только мы, но и сотрудники банковской организации, а также, возможно, лица, обслуживающие автоматизированную банковскую систему, и аудиторы.

Действия со счетом могут быть санкционированными (например, мы переводим денежные средства с одного счета на другой, оператор просматривает информацию нашего счета при проведении операции) и несанкционированными (например, стороннее лицо осуществляет перевод денежных средств с нашего счета, но без нашего ведома). Если мы можем противостоять несанкционированным изменениям информации, то говорят, что мы обеспечиваем ее **целостность**.

**Определение 1.3.** *Целостность информации — это состояние информации, при котором отсутствует любое ее изменение или изменение осуществляется только преднамеренно субъектами, имеющими необходимые права.*

И последнее основное свойство безопасности — **доступность**.

Каждый из нас хотя бы один раз оказывался в ситуации, при которой информация необходима нам немедленно. Например, нам требуется связаться с родственником, попавшим в сложную жизненную ситуацию, или срочно необходимо оплатить покупку. Доступность информации оказывается критичной во многих ситуациях, требующих немедленного реагирования, например, в случае работы станка, обрабатывающего сложную деталь и получающего управляющие команды в режиме реального времени, или в случае игры на бирже, при которой необходимо как можно более оперативно реагировать на изменяющуюся ситуацию.

**Определение 1.4.** *Доступность информации — это состояние информации, при котором лицу, обладающему правом доступа к информации и выполнившему все необходимые условия для получения доступа к информации и ее использованию, не может быть отказано в доступе.*

Обратим внимание на ограничения, приведенные в определении.

Во-первых, доступность информации гарантируется только лицу, которое легитимно обращается к информации, то есть имеет право получить запрашиваемую информацию. Можно сказать, что одной из задач защиты информации является создание таких условий, при которых время получения информации при несанкционированном обращении должно стремиться к бесконечности.

Во-вторых, даже если Вы обладаете правом на получение информации, одного желания ее получить недостаточно. Требуется также соблюдение всех необходимых условий.

Например, для получения информации о банковском счете мы должны не просто обратиться к автоматизированной банковской системе посредством приложения «клиент-банк», но и должны предъявить определенную информацию,

идентифицирующую нас в этой системе (обычно логин, пароль и одноразовый код, приходящий по альтернативному каналу связи и подтверждающий наше знание об этом канале и владение определенным устройством). Или для закрытия нашего счета в банке необходимо не только прийти в банк, но и подтвердить нашу личность, предъявив паспорт и, возможно, другие документы.

### 1.3. Классификация информации по возможности доступа и с точки зрения возможности распространения

Как мы уже знаем, не ко всякой информации мы можем получить доступ. Например, мы можем получить доступ к состоянию своего банковского счета, но не можем получить доступ к банковскому счету стороннего лица.

В нашем законодательстве в зависимости от категории доступа выделяют **общедоступную** информацию и информацию, **доступ к которой ограничен федеральными законами** (информацию **ограниченного доступа**).

Как следует из названия, к **общедоступной** информации доступ может получить каждый. Для получения доступа к информации **ограниченного доступа** необходимо удовлетворять определенным требованиям (например, быть ее обладателем или входить в круг лиц, имеющих право доступа к такой информации).

К общедоступной информации относятся общеизвестные сведения (например, правила сложения и умножения целых чисел) и иная информация, доступ к которой не ограничен (например, список книг в общественной библиотеке). Общедоступная информация может использоваться любыми лицами по их усмотрению при условии, что они соблюдают правила распространения такой информации, установленные федеральными законами.

Особо выделяется ряд сведений, доступ к которым в соответствии с нашим законодательством нельзя ограничивать. Примерами таких сведений выступают [5]:

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина;
- информация о деятельности государственных органов и органов местного самоуправления;
- информация о состоянии окружающей среды;
- сведения об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информация, накапливаемая в открытых фондах библиотек, музеев и архивов (в том числе оцифрованная).

Ограничить доступ к произвольной информации, исходя только из своего желания, нельзя. Ограничение доступа к отдельным видам информации устанавливается федеральными законами. Примеров таких законов достаточно много. Помимо трех законов, непосредственно посвященных особым видам информации ограниченного доступа: государственной тайне, коммерческой тайне и персональным данным, — существует множество законов, вводящих различные профессиональные тайны.

Для иллюстрации широты охвата, приведем далеко не полный перечень таких тайн: налоговая тайна, банковская тайна, тайна страхования, тайна ломбарда, адвокатская

тайна, тайна завещания, тайна следствия, тайна совещания судей, врачебная тайна, тайна связи, тайна усыновления и тайна исповеди. При этом следует отметить, что многие из перечисленных тайн также являются персональными данными.

Обратим внимание на следующее важное положение: соблюдение конфиденциальности информации является обязательным в том случае, если доступ к ней ограничен федеральными законами.

В связи с этим представляет интерес вопрос о статусе «информации для служебного пользования» (или служебной информации ограниченного распространения). До сих пор на некоторых документах можно встретить метку «для служебного пользования», что должно предупреждать о наличии в документе конфиденциальной информации, предназначенной для ознакомления или использования только в служебных целях.

Однако федерального закона «О служебной информации» не существует. Он разрабатывался параллельно с Федеральным законом «О персональных данных» в 2008 году, но не был принят Государственной Думой. На текущий момент документом, определяющим порядок обработки и защиты служебной информации ограниченного распространения, является Постановление Правительства РФ от 03.11.1994 №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности», статус которого ниже, чем статус федерального закона. Поэтому правовой статус документов, имеющих метку «для служебного пользования», во многом является дискуссионным.

Заметим также, что конфиденциальность не является единственным свойством информации, которое необходимо обеспечить, поэтому существуют достаточно много видов информации, требующих защиты, но не требующих ограничения доступа. В частности, защиты требуют открытые и общедоступные ресурсы (например, официальные сайты органов государственной власти и организаций), сведения, влияющие на работу автоматизированных систем управления технологическими процессами (например, сведения о температуре окружающей среды или давлении) и другая информация.

Если доступ к информации ограничивается, «... значит — это кому-нибудь нужно». В первую очередь, ограничение доступа к информации призвано обеспечить преимущество одних лиц перед другими, основывающееся на возможности использования такой информации. Здесь возникает один из главных субъектов (российского законодательства) в сфере обработки и защиты информации — владелец или обладатель информации.

**Определение 1.5.** *Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.*

Обладателями информации могут выступать: физические лица, юридические лица, а также Российская Федерация, субъект Российской Федерации или муниципальное образование. В трех последних случаях право разрешать или ограничивать доступ к информации реализуется органами государственной власти и местного самоуправления, на которые возложены соответствующие полномочия.

Обладатель информации реализует всю полноту прав в ее отношении. В частности, он имеет права на использование информации по своему усмотрению (в том числе на уничтожение информации, ее дарение, продажу и т. п.), на ограничение доступа



к информации, на защиту (законными способами) своих прав на информацию в случае их нарушения. При этом обладатель информации обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации, а также ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Классифицируя информацию по порядку доступа, мы смотрим на нее с точки зрения получателя. Теперь мы рассмотрим вопрос о классификации информации с точки зрения источника. Для начала отметим, что наше законодательство выделяет два формата передачи информации: **предоставление** и **распространение**.

**Определение 1.6.** *Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.*

**Определение 1.7.** *Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.*

Обратим внимание, что это достаточно важно, поскольку многие вопросы об ответственности сформулированы в терминах только одного формата передачи информации и вопрос об ответственности применительно ко второму формату является дискуссионным. Например, в части 1 статьи 242 Уголовного кодекса Российской Федерации «Незаконные изготовление и оборот порнографических материалов или предметов» состав преступления сформулирован следующим образом:

*Незаконные изготовление и (или) перемещение через Государственную границу Российской Федерации в целях **распространения**, публичной демонстрации или рекламирования либо **распространение**, публичная демонстрация или рекламирование порнографических материалов или предметов.*

Итак, в зависимости от порядка распространения (предоставления) выделяют следующие виды информации [5]:

1. Свободно распространяемая информация (например, перечень книг в публичной библиотеке);
2. Информация, предоставляемая по соглашению лиц, участвующих в определенных отношениях (например, произведения, защищенные авторским правом);
3. Информация, подлежащая предоставлению или распространению (например, сведения о золотовалютных резервах Российской Федерации);
4. Информация, распространение которой в Российской Федерации ограничивается или запрещается.

Например, на территории Российской Федерации запрещается распространение [5]:

1. *Информации, направленной на пропаганду войны.*
2. *Информации, направленной на разжигание национальной, расовой или религиозной ненависти и вражды.*
3. *Информации, за распространение которой предусмотрена уголовная или административная ответственность (например, государственная тайна).*

## 1.4. Информационные технологии и информационные системы

Следующим важным понятием, определение которому дано в Федеральном законе «Об информации, информационных технологиях и о защите информации» является понятие «информационные технологии».

**Определение 1.8.** *Информационные технологии — это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.*

Это определение также является достаточно общим. В рамках данного определения информационными технологиями оказываются, например, чтение газет, объявлений, формирование библиотек (бумажных и электронных книг), распространение листовок, рассылка электронных писем, хранение информации в центрах обработки данных, обработка видео на компьютере, общение через смс и сервисы обмена мгновенными сообщениями, передача информации по спутниковым каналам связи и многое-многое другое.

Как мы уже знаем, информация не существует сама по себе. С одной стороны, обязательно должен существовать носитель информации. С другой стороны, должны быть определены информационные технологии, которые позволяют работать с информацией на таком носителе. В противном случае, само по себе существование информации без возможности ее использования (применения) может не оказывать на нас никакого влияния.

При этом можно привести примеры ситуаций, при которых информация (вместе с носителем) существует, но технологий, позволяющих извлечь эту информацию и работать с ней, еще не существует. Например, можно считать, что наша Вселенная является «носителем» информации о самой себе. Поэтому открытие нового физического закона, по сути, является актом извлечения существовавшей на «носителе» информации, которую до этого момента не могли извлечь.

Другим примером является невозможность (по крайней мере на текущий момент) чтения человеческих мыслей, если только человек сам их не воспроизводит. Поэтому студентам приходится доказывать преподавателям, что они что-то знают путем непосредственного воспроизведения своих мыслей.

Итак, с учетом сказанного, введем в рассмотрение еще одно важное понятие — «информационная система».

**Определение 1.9.** *Информационная система (ИС) — это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.*

Информационную систему можно рассматривать как основной «строительный» элемент и «учетную единицу» в сфере информатизации и информационных технологий. Можно сказать, что нас окружают информационные системы, это не только широко известные Портал государственных услуг, Единая государственная информационная система в сфере здравоохранения или Единый государственный реестр записей актов гражданского состояния, но и информационные системы предприятий — кадровые или бухгалтерские информационные системы, системы управления предприятием (ERP) или системы управления взаимоотношениями с клиентами (CRM). Более того, у каждого из нас есть, как минимум, одна своя информационная система, например, телефонный справочник друзей и знакомых.

Вернемся к определению информационной системы. Обратим внимание, что приведенное определение уже не подразумевает рассмотрение любой информации независимо от формы ее представления.

Согласно статье 1260 Гражданского кодекса Российской Федерации **базой данных** является представленная в **объективной форме** (соответственно мысли человека не попадают под определение) совокупность самостоятельных материалов (например, статей, расчетов и т. п.), **систематизированных** таким образом, чтобы эти материалы могли быть **найжены и обработаны с помощью электронной вычислительной машины**.

Соответственно, говоря об информационной системе, мы подразумеваем не только применение компьютеров для обработки информации, но и обязательно определенные свойства самой обрабатываемой информации, а именно пригодность для обработки с помощью компьютера (объективную форму) и наличие определенной структуры (системности).

Несмотря на вышесказанное, под приведенное определение информационной системы попадает все еще очень широкий класс объектов. Например, в состав информационной системы могут входить базы данных с системами управления, такие как Oracle, MS SQL или MySQL, а могут электронные таблицы Excel. Более того, структурированная таблица в файле формата Microsoft Word также может рассматриваться в качестве базы данных и вместе с программным обеспечением и компьютером, на котором хранится файл, она формирует информационную систему.

Круг возможных технических средств, входящих в состав информационной системы, также очень широк. Примерами технических средств являются серверы, персональные компьютеры, ноутбуки и планшеты, смартфоны, коммутационное оборудование, принтеры, веб-камеры и многое другое.

Таким образом, примерами информационных систем могут являться и упорядоченный перечень слушателей этого курса в файле формата Microsoft Word на рабочем компьютере преподавателя, и система управления университетом, включающая серверы, рабочие места пользователей — сотрудников университета и уже упомянутый Портал государственных услуг, в состав которого входят несколько центров обработки данных, а круг пользователей потенциально не ограничен.

Принято выделять три вида информационных систем.

К первому виду относятся государственные информационные системы, созданные на основании федеральных законов, законов субъектов Российской Федерации или на основании правовых актов государственных органов. По масштабу государственные информационные системы делятся на региональные, территориально расположенные в одном субъекте Российской Федерации, и федеральные, территориально расположенные в нескольких субъектах Российской Федерации или на территории всей Российской Федерации.

Ко второму виду относятся муниципальные информационные системы, созданные на основании решения органа местного самоуправления. Такие информационные системы обычно расположены в пределах одного города или района субъекта Российской Федерации.

Все остальные информационные системы относятся к третьему виду «иных информационных систем». Такими информационными системами являются информационные системы предприятий и организаций, частные информационные системы независимо от их территориального размещения. Например, информационные

системы ПАО «Газпром», социальная сеть ВКонтакте и наш телефонный справочник в телефоне относятся к иным информационным системам.

Обратим внимание, что, несмотря на правовое закрепление приведенной классификации, существуют альтернативные взгляды на то, что считать государственными информационными системами. Например, в одном из основных альтернативных подходов предлагается считать государственными все информационные системы, создание которых финансировалось (или финансируется) из бюджетов федерального и регионального уровней, при этом наличие правовых актов не считается первостепенным.

Поскольку информационная система содержит в своем составе технические средства, а также программное обеспечение, реализующее информационные технологии, то кто-то должен поддерживать их в работоспособном состоянии, обновлять, модернизировать, заменять и т. п. Лицо, обслуживающее информационную систему, принято называть **оператором информационной системы**. Это второй по важности (после обладателя информации) субъект в сфере информатизации и информационных технологий. Приведем формальное определение.

**Определение 1.10.** *Оператор информационной системы — это гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.*

Обладатель информации и оператор информационной системы могут находиться в различных отношениях. Эти роли могут совпадать или быть различными. К примеру, мы являемся обладателем информации в нашем смартфоне и одновременно оператором телефонного справочника. С другой стороны, мы можем являться обладателями информации, но поручить ее эксплуатацию центру обработки данных, который будет выступать в данном случае в роли оператора.

Более того, роли обладателя и оператора могут быть распределены между несколькими лицами. Например, технические средства центра обработки данных может арендовать организация, которая развернет на них информационную инфраструктуру социальной сети, к которой уже будут подключаться пользователи — обладатели «страниц» в этой социальной сети.

Необходимо отметить, что могут возникать и достаточно парадоксальные ситуации. Например, как обладатель информации, размещаемой на нашей странице в социальной сети, мы можем разрешать и ограничивать доступ к ней, но владелец самой социальной сети также может ограничить доступ к нашей странице и размещенной на ней информации, в том числе и нам самим.

То же самое может произойти во втором приведенном примере, в ситуации, при которой центр обработки данных (например, за неуплату) может ограничить доступ к информации ее обладателю. Поэтому в общем случае определение того, у кого в конкретный момент времени может оказаться больше прав на информацию (и ресурсов на их реализацию) у обладателя или у оператора, может оказаться достаточно трудной задачей.

В случаях, при которых роль оператора информационной системы не определена явно (например, она может быть прописана в правовых документах, являющихся основанием для создания информационной системы), оператором информационной системы считается **собственник технических средств**, которые используются для обработки содержащейся в базах данных информации (обратим внимание, что такой подход исключает, например, собственника коммутационного оборудования

и вспомогательных технических средств), или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы (отметим, что таких договоров может быть несколько, например, эксплуатация различных компонентов информационной системы может осуществляться различными организациями).

Обладатель информации и оператор информационной системы в случаях, если это установлено законодательством Российской Федерации, обязаны принимать **правовые, организационные и технические** меры по защите информации, направленные на [5]:

- предотвращение неправомерного (несанкционированного) доступа к информации, результатом которого может стать уничтожение, модификация, блокирование, копирование, предоставление или распространение информации, а также любые другие неправомерные действия в ее отношении;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию прав доступа к информации.

В случаях, установленных законодательством Российской Федерации, обладатель информации и оператор информационной системы обязаны обеспечить [5]:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим прав доступа к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

На настоящий момент в нормативно-правовой базе Российской Федерации можно выделить следующие основные виды защищаемой информации и основные виды защищаемых информационных систем (объекты защиты):

- государственная тайна;
- персональные данные;
- коммерческая тайна;
- информация для служебного пользования (смотри замечание о статусе этого вида конфиденциальной информации в разделе «Классификация информации по возможности доступа и возможности распространения»);
- объекты критической информационной инфраструктуры;

- государственные информационные системы;
- информационные системы персональных данных;
- автоматизированные системы управления технологическими процессами;
- открытые и общедоступные информационные ресурсы.

По каждому представленному в предыдущем списке объекту защиты существует своя «ветвь» в законодательстве Российской Федерации, в которую в том числе входят ведомственные правовые документы Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, устанавливающие требования к составу и содержанию мер по защите информации.

## 1.5. Ответственность в сфере обработки и защиты конфиденциальной информации

Нарушение требований федерального законодательства в сфере обработки и защиты конфиденциальной информации может повлечь различные виды ответственности. Правилами внутреннего трудового распорядка организаций и предприятий может предусматриваться **дисциплинарная** ответственность (за совершение дисциплинарного проступка работодатель может применить к работнику дисциплинарное взыскание: замечание, выговор или увольнение). Серьезные проступки могут являться **административными правонарушениями** или **преступлениями**.

Основными нормативными правовыми актами, определяющими ответственность в сфере обработки и защиты конфиденциальной информации, являются Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) и Уголовный кодекс Российской Федерации (УК РФ). Рассмотрим их более подробно<sup>1</sup>.

Основные правонарушения в области обработки конфиденциальной информации предусматриваются статьями 13.11 «Нарушение законодательства Российской Федерации в области персональных данных» и 13.14 «Разглашение информации с ограниченным доступом» КоАП РФ.

Объектом правонарушения, предусмотренного статьей 13.11 КоАП РФ, являются общественные отношения, возникающие при обработке ПДн, а также при исполнении оператором возложенных на него законодательством Российской Федерации обязанностей и законных требований субъектов ПДн. Субъектами правонарушения могут являться граждане, должностные и юридические лица. Объективная сторона правонарушения состоит в действии или бездействии, приводящем к нарушению порядка обработки ПДн и исполнения оператором своих обязанностей и законных требований субъектов ПДн.

Объектом правонарушения, предусмотренного статьей 13.14 КоАП РФ, являются общественные отношения, возникающие при обработке информации ограниченного доступа. Субъектами правонарушения в этом случае могут являться граждане, получившие доступ к информации ограниченного доступа в связи с исполнением служебных или профессиональных обязанностей. Объективная сторона

---

<sup>1</sup>Основано на комментариях к КоАП РФ, приведенных на сайтах <http://koapkodeksrf.ru/>, <https://kodeks.ru/news/read/podgotovlen-novyy-postateyny-kommentariy-k-koap-rf>, и комментариях к УК РФ, приведенных на сайтах <http://ukodeksrf.ru/>, <http://stykrf.ru/>.

правонарушения состоит в действии или бездействии, приводящем к разглашению информации ограниченного доступа (то есть передаче, предоставлению или распространению информации ограниченного доступа лицам, не имеющим права доступа к ней). При этом, если разглашение информации ограниченного доступа образует состав преступления, то лицо, его совершившее, будет нести уголовную, а не административную ответственность.

С точки зрения обработки конфиденциальной информации близкой к статьям 13.11 и 13.14 КоАП РФ является статья 5.27 КоАП РФ «Нарушение трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права», поскольку вопросы обработки ПДн работников регулируются Трудовым кодексом Российской Федерации. Объектом правонарушений, предусмотренных частями 1 и 2 статьи 5.27 КоАП РФ, являются общественные отношения, возникающие в сфере трудового права, в частности к объекту правонарушения можно отнести общественные отношения, возникающие при обработке работодателем ПДн работников. Объективная сторона правонарушений состоит в действии или бездействии, приводящем к невыполнению или нарушению норм действующего трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, в том числе нарушению порядка обработки ПДн работников. Субъектом правонарушения, предусмотренного частью 1 статьи 5.27 КоАП РФ, является, должностное лицо (например, работодатель или представитель работодателя) или лицо, осуществляющее предпринимательскую деятельность без образования юридического лица, а субъектом правонарушения, предусмотренного частью 2 той же статьи, — лицо, которое ранее подвергалось наказанию за аналогичное правонарушение.

Статьи 13.12 «Нарушение правил защиты информации» и 13.13 «Незаконная деятельность в области защиты информации» КоАП РФ определяют основные составы административных правонарушений в области защиты конфиденциальной информации. Объектом правонарушений, предусмотренных указанными статьями, являются общественные отношения, возникающие при осуществлении деятельности в области защиты информации.

Статья 13.12 КоАП РФ содержит семь составов правонарушений, части 3, 4 и 7 указанной статьи предусматривают ответственность за неправомерные действия при защите сведений, составляющих государственную тайну, и поэтому здесь не рассматриваются.

Объективная сторона правонарушений, предусмотренных частями 1 и 5 статьи 13.12 КоАП РФ, состоит в действии или бездействии, приводящем, соответственно, к нарушению и грубому нарушению условий, предусмотренных лицензией на осуществление деятельности по защите информации. Субъектами административных правонарушений в первую очередь являются юридические лица или индивидуальные предприниматели, имеющие лицензию на осуществление деятельности в области защиты информации, а также должностные лица.

Примером нарушения при осуществлении лицензируемой деятельности по технической защите конфиденциальной информации является нарушение сроков повышения квалификации сотрудников организации-лицензиата, непосредственно принимающих участие в оказании услуг по технической защите конфиденциальной информации, а также лиц, руководящих этой деятельностью.

Примером грубого нарушения в соответствии с пунктом 7 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного Постановлением Правительства Российской Федерации от 03.02.2012

№ 79, является использование при оказании услуг по технической защите конфиденциальной информации измерительных приборов (прошедших в установленном законодательством Российской Федерации порядке метрологическую поверку), не принадлежащих лицензиату на праве собственности или ином законном основании.

Объективная сторона правонарушения, предусмотренного частью 2 статьи 13.12 КоАП РФ, состоит в действии или бездействии, приводящем к использованию несертифицированных средств защиты информации, а также иного несертифицированного программного обеспечения и баз данных. Субъектами административного правонарушения в этом случае могут быть граждане, а также должностные и юридические лица.

Наконец, объективная сторона правонарушения, предусмотренного частью 6 рассматриваемой статьи, состоит в действии или бездействии, приводящем к нарушению требований о защите информации, установленных федеральными законами, и принятыми в соответствии с ними подзаконными актами. Например, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Субъектами административного правонарушения в этом случае также могут являться граждане, должностные и юридические лица.

В отличие от правонарушений, предусмотренных частями 1 и 5 статьи 13.12 КоАП РФ, объективная сторона правонарушения, предусмотренного частью 1 статьи 13.13 КоАП РФ, состоит в действии, направленном на осуществление деятельности в области защиты информации без необходимой для осуществления такой деятельности лицензии. Субъектами правонарушения в этом случае могут быть граждане, а также должностные и юридические лица. Часть 2 указанной статьи предусматривает ответственность за аналогичные действия, связанные с использованием и защитой сведений, составляющих государственную тайну, и поэтому здесь не рассматривается.

Отдельную группу статей КоАП РФ, определяющих меры ответственности за нарушения в области обработки и защиты конфиденциальной информации, составляют статьи, в которых объектом правонарушения являются общественные отношения, возникающие при осуществлении государственного контроля или надзора, в том числе в области обработки и защиты информации. Примерами таких статей КоАП РФ являются:

1. Статья 19.4 «Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль), должностного лица организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора, должностного лица органа, осуществляющего муниципальный контроль».
2. Статья 19.4.1 «Воспрепятствование законной деятельности должностного лица органа государственного контроля (надзора), должностного лица организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора, должностного лица органа муниципального контроля».
3. Статья 19.5 «Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора (должностного лица), органа (должностного лица), осуществляющего муниципальный контроль».



4. Статья 19.6 «Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения».
5. Статья 19.7 «Непредставление сведений (информации)».

Обратим внимание на статью 19.7 КоАП РФ. Сбор уполномоченными органами государственной власти информации является одним из методов осуществления государственного контроля. Например, часть 4 статьи 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» устанавливает, что оператор (персональных данных) обязан сообщить по запросу уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзора) всю необходимую информацию. Объективная сторона правонарушения, предусмотренного статьей 19.7 КоАП РФ, состоит в действии или бездействии, приводящем к непредоставлению или несвоевременному предоставлению информации в уполномоченный орган, а также к предоставлению информации в неполном или искаженном виде. Субъектами административного правонарушения могут выступать граждане, должностные и юридические лица.

Перейдем к рассмотрению положений Уголовного кодекса Российской Федерации. С развитием информационных технологий растет число видов преступлений, связанных с обработкой и защитой информации. Примерами преступлений являются кража идентификационных данных (например, логинов и паролей, PIN-кодов), реквизитов банковских карт, паспортных данных, создание подложных (мошеннических) сайтов, незаконное воздействие на информационную инфраструктуру, способное нарушить штатное функционирование информационных систем и автоматизированных систем управления технологическими процессами. Каждое из перечисленных преступлений может привести к существенному (как материальному, так и моральному) ущербу для гражданина, общества или государства. Здесь мы рассмотрим только ряд примеров преступлений в сфере обработки и защиты информации.

Объектом преступлений, предусмотренных статьями 137 «Нарушение неприкосновенности частной жизни» и 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, являются общественные отношения, возникающие при реализации конституционных прав граждан на неприкосновенность частной жизни, личной и семейной тайны и на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений соответственно. Субъектами преступлений, предусмотренными частями 1 и 3 статьи 137 УК РФ и части 1 статьи 138 УК РФ, являются вменяемые физические лица, достигшие (к моменту совершения преступления) возраста 16 лет. Субъектами преступлений, предусмотренными частью 2 статьи 137 УК РФ и частью 2 статьи 138 УК РФ, являются лица, использующие при совершении преступления свое служебное положение. Объективная сторона преступлений, предусмотренных частями 1 и 2 статьи 137 УК РФ, состоит в действии, направленном на незаконный сбор или распространение (в том числе, в публичном выступлении, публично демонстрирующемся произведении или СМИ) сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия. Объективная сторона преступления, предусмотренного частью 3 рассматриваемой статьи, состоит в действии, направленном на распространение сведений о жертвах преступлений (потерпевших), не достигших возраста 16 лет, следствием которого являются тяжкие последствия для потерпевших. Объективная сторона преступлений, предусмотренных статьями 138 УК РФ, состоит в действии,

направленном на нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Объектом преступления, предусмотренного статьей 140 «Отказ в предоставлении гражданину информации» УК РФ, являются общественные отношения, возникающие в связи с конституционной обязанностью органов государственной власти и органов местного самоуправления, а также их должностных лиц, обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы (часть 2 статьи 24 Конституции Российской Федерации). Субъектом преступления является должностное лицо. Объективная сторона преступления состоит в действии или бездействии, приводящем к неправомерному отказу в предоставлении информации, непосредственно затрагивающей права и свободы гражданина, а также в предоставлении неполной или заведомо ложной информации, в случае, если это привело к причинению вреда правам и законным интересам граждан.

Объектом преступления, предусмотренного статьей 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, являются общественные отношения, возникающие вследствие применения информационных технологий. Субъектом преступления является вменяемое физическое лицо, достигшее возраста 16 лет. Объективная сторона преступления состоит в действии, направленном на хищение чужого имущества или приобретение права на него с помощью применения информационных технологий и обработки информации (путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей). Признаками, характеризующими мошенничество в сфере компьютерной информации, как деяние, обладающее повышенной общественной опасностью, являются совершение преступления группой лиц по предварительному сговору, а равно с причинением значительного ущерба потерпевшему, совершение преступления лицом с использованием своего служебного положения, с причинением ущерба в крупном размере или с причинением ущерба в отношении банковского счета или электронных денежных средств, совершение преступления организованной группой либо с причинением ущерба в особо крупном размере.

Объектом преступления, предусмотренного статьей 272 «Неправомерный доступ к компьютерной информации» УК РФ, являются общественные отношения, возникающие при обеспечении свойств безопасности информации (в первом приближении, конфиденциальности, целостности и доступности). Субъектом преступления является вменяемое физическое лицо, достигшее возраста 16 лет. Объективная сторона преступления состоит в действии, направленном на осуществление неправомерного доступа к охраняемой законом компьютерной информации (например, персональным данным, коммерческой тайне и т. п.), если это действие повлекло несанкционированное уничтожение, блокирование, модификацию или копирование информации (то есть нарушение свойств безопасности информации). Признаками, характеризующими неправомерный доступ к компьютерной информации, как деяние, обладающее повышенной общественной опасностью, являются причинение крупного ущерба или совершение преступления из корыстной заинтересованности, совершение преступления группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, совершение преступления повлекшего тяжкие последствия или создавшего угрозу их наступления.

В заключение отметим, что кроме КоАП РФ и УК РФ, ответственность в области обработки и защиты информации могут определять и другие правовые документы. Например, в соответствии со статьей 81 Трудового кодекса Российской Федерации:

*Работодатель может в одностороннем порядке расторгнуть трудовой договор в случае, если сотрудник разгласил охраняемую законом тайну, ставшую известной работнику в связи с исполнением им трудовых обязанностей.*

## 1.6. Вопросы и задания

1.1. Дайте определение понятию «информация».

1.2. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?

1.3. Какие виды информации обязательно требуется защищать в соответствии с законодательством Российской Федерации?

1.4. Что из перечисленного можно рассматривать как базу данных в соответствии с законодательством Российской Федерации?

1. EXCEL таблицу с упорядоченной и структурированной информацией.
2. Файл формата DOC, в котором создан список слушателей этой программы.
3. Картотеку регистратуры учреждения здравоохранения.
4. Все перечисленное.

1.5. Дайте определения понятиям «конфиденциальность информации», «целостность информации», «доступность информации».

1.6. Выберите верные утверждения. На территории Российской Федерации запрещено распространение:

1. Информации, которая направлена на пропаганду войны.
2. Коммерческой тайны.
3. Информации, которая направлена на разжигание религиозной ненависти.
4. Персональных данных.

1.7. Дайте определения понятиям «обладатель информации» и «оператор информационной системы».

1.8. Кто является оператором информационной системы?

1. Обладатель информации.
2. Собственник используемых для обработки содержащейся в базах данных информации технических средств.
3. Лицо, определяющее цели обработки информации и осуществляющее обработку информации.

1.9. Приведите примеры видов информации, к которой (в соответствии с законодательством Российской Федерации) не может быть ограничен доступ.

1.10. Какие виды ответственности может повлечь нарушение требований федеральных законов в области обработки и защиты информации?

## 2. Защита персональных данных

### 2.1. Правовые акты в области обработки и защиты персональных данных

На текущий момент в Российской Федерации действует большой комплекс правовых и методических документов, регламентирующих обработку и защиту персональных данных (ПДн). В таблице 1 приводятся наименования двенадцати основных документов, а также назначение каждого из них.

Таблица 1.

Правовые акты в сфере обработки и защиты персональных данных

№	Наименование документа	Назначение документа
1	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	Основной федеральный закон, регулирующий вопросы обработки и защиты персональных данных. Содержит основные термины и определения, устанавливает права граждан, а также права и обязанности лиц, обрабатывающих персональные данные, и органов государственной власти, осуществляющих контроль и надзор в сфере обработки и защиты персональных данных
2	Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	Содержит порядок определения уровня защищенности персональных данных. Уровень защищенности является основой для выбора мер защиты персональных данных, в соответствии с 21-м приказом ФСТЭК России
3	Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»	Уточняет и расширяет требования Федерального закона «О персональных данных» в отношении операторов персональных данных, являющихся органами государственной власти и местного самоуправления

<b>№</b>	<b>Наименование документа</b>	<b>Назначение документа</b>
4	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»	Регулирует отношения, связанные с обработкой персональных данных без использования средств вычислительной техники, то есть при их неавтоматизированной обработке
5	Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»	Определяет порядок обработки биометрических персональных данных. Актуально, например, для биометрических паспортов нового поколения
6	Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»	Описывает порядок уведомления Роскомнадзора (органа государственной власти, уполномоченного по вопросам защиты прав субъектов персональных данных) о начале обработки организацией персональных данных и порядок внесения изменений в ранее предоставленные сведения
7	Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»	Устанавливает требования к процедурам обезличивания персональных данных, обрабатываемых в органах государственной власти и местного самоуправления
8	Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	Один из важнейших технических документов. Определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных без использования средств криптографической защиты информации
9	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год	Содержит классификацию и описание основных угроз информационной безопасности, а также типовые наборы актуальных угроз для определенных типов информационных систем

№	Наименование документа	Назначение документа
10	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год	Определяет порядок оценки актуальности угроз информационной безопасности для конкретной информационной системы с учетом ее функциональных особенностей
11	Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состав 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»	Определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации
12	Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432	Описывает порядок определения класса средств криптографической защиты информации. Всего выделяют пять классов средств криптографической защиты информации (КС1, КС2, КС3, КВ и КА). Каждый класс обеспечивает безопасность относительно определенного вида нарушителей

Обратим внимание, что в некоторых ситуациях представленный перечень документов потребует дополнения. Например, при обработке ПДн в государственных информационных системах, мы обязаны исполнять не только требования законодательства о защите ПДн, но и требования по защите государственных информационных систем.

Кроме того, в отдельных случаях при обработке ПДн необходимо учитывать требования международных нормативных правовых актов. Например, регламент обработки ПДн граждан Европейского Союза призван обеспечить безопасность таких ПДн независимо от того, на территории какой страны они обрабатываются. Этот регламент исходит из глобальности мирового рынка и возможности масштабной передачи ПДн граждан Европейского Союза на территории других государств в целях продвижения товаров и услуг. Отметим, что в этой части подход, находящий отражение в нашем законодательстве, существенно отличается от подхода Европейского Союза. В

нашем законодательстве выражено стремление к локализации обработки ПДн граждан Российской Федерации на территории нашей страны.

В случаях, при которых Вы организуете или осуществляете обработку ПДн иностранных граждан, Вы должны учитывать возможность существования требований иностранных государств относительно обработки ПДн их граждан. Эти ситуации отнюдь не редки, например, обработка ПДн иностранных граждан осуществляется в сферах туризма, транспорта и гостиничного бизнеса.

Как мы уже знаем, основным правовым документом, регламентирующим обработку и защиту ПДн на территории Российской Федерации, является Федеральный закон «О персональных данных». При этом он во многом базируется на Конституции Российской Федерации и Федеральном законе «Об информации, информационных технологиях и о защите информации», положения которых мы рассматривали ранее.

Федеральный закон «О персональных данных» регулирует отношения, связанные с обработкой ПДн, в независимости от того, кто ее осуществляет. Например, обрабатывать персональные данные могут органы государственной власти различных уровней, органы местного самоуправления и подведомственные им организации, иные юридические и физические лица. Для всех перечисленных лиц в отношении обработки и защиты ПДн действуют одни и те же основные правовые нормы.

Обратим внимание, что Федеральный закон «О персональных данных» регулирует не только отношения, связанные с автоматизированной обработкой ПДн (то есть обработкой с использованием средств вычислительной техники), но и отношения, при которых обработка ПДн ведется без использования средств автоматизации в случае, если порядок такой обработки «схож» с порядком обработки ПДн с использованием средств автоматизации.

Последняя ситуация до сих пор часто встречается, например, в регистратурах учреждений здравоохранения, в которых медицинские карты пациентов хранятся в картотеках или систематизированных собраниях. Несмотря на архаичность, такая организация хранения позволяет реализовать алгоритмы поиска медицинских карт по фамилии, имени и отчеству пациента или по специальному идентификатору.

Важно учитывать, что действие Федерального закона «О персональных данных» не распространяется на следующие отношения [6]:

1. Отношения, возникающие при обработке ПДн физическими лицами исключительно для личных и семейных нужд.

Например, обработку ПДн Ваших друзей на Вашем личном телефоне Федеральный закон «О персональных данных» не регулирует.

2. Отношения, возникающие при обработке информации в соответствии с законодательством об архивном деле в Российской Федерации.

В данном случае важно соблюдать аккуратность. Законодательство Российской Федерации об архивном деле предусматривает формирование архивных дел, организацию их учета и хранения в специальных помещениях, а также выдачу архивных дел под роспись в специальном журнале, с обязательным последующим возвращением. До настоящего момента в законодательстве Российской Федерации фактически нет определения понятия «архив в электронном виде».

3. Отношения, связанные с обработкой ПДн, составляющих государственную тайну. В этой ситуации персональные данные защищаются как более важный вид информации, в соответствии с законом «О государственной тайне».

## 2.2. Обработка персональных данных. Основные понятия и их определения

Наверняка Вам уже интересно, что же такое «персональные данные»?

**Определение 2.1.** *Персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).*

Вокруг этого определения сломано достаточно большое число копий, поскольку во многих ситуациях очень сложно определить границу между тем, что ещё является персональными данными, и тем, что персональными данными уже не является.

Ясно, что, указывая однозначные идентификаторы субъекта ПДн (например, его паспортные данные, СНИЛС, реквизиты водительского удостоверения) или неполные идентификаторы и дополнительную информацию (например, фамилию, имя отчество, место работы и должность или фамилию, имя, отчество и адрес проживания), мы можем однозначно идентифицировать субъекта. Поэтому эти сведения, безусловно, являются персональными данными.

Однако достаточно часто возникают ситуации, при которых очень трудно сделать однозначный вывод о том, можно ли определить субъекта ПДн по имеющейся информации. Например, можно ли однозначно определить субъекта только по имени, фамилии и отчеству? С одной стороны, если мы говорим об Иванове Иване Ивановиче, то таких людей на территории Российской Федерации достаточно много и сложно сказать, о ком конкретно идёт речь (однако для небольшого поселка ситуация может быть иной!). С другой стороны, если мы говорим, например, об Иосифе Виссарионовиче Сталине, то контекст возникает непосредственно из фамилии, имени и отчества человека.

Поэтому, с нашей точки зрения, любые сомнения должны трактоваться в пользу субъектов ПДн.

Помимо «классических» ПДн (таких как, паспортные данные, сведения об образовании, сведения о состоянии здоровья и т. п.) существенное значение приобретают ПДн, связанные с обработкой «больших данных». Значительная часть таких ПДн создается в процессе взаимодействия субъекта с различными «умными» устройствами, например, обычными персональными компьютерами или смартфонами, но возможно «умным холодильником» или турникетом в метрополитене. Примерами таких ПДн являются геолокационные данные, отслеживаемые операторами сотовой связи по траекториям движения сотовых телефонов, сведения о вызывающих интерес сайтах или потенциально интересных товарах, собираемые и обрабатываемые поисковыми системами, данные о Вашей активности на сайтах и о регулярности оплаты счетов, статистика посещения магазинов, а также сведения о «среднем чеке» и многое-многое другое.

**Определение 2.2.** *Под обработкой персональных данных понимаются любые действия с персональными данными, совершаемые с использованием средств автоматизации или без использования таких средств.*

Обратим внимание, что хранение ПДн включается в обработку. Поэтому факт наличия (в организации) ПДн на материальных носителях уже говорит об их обработке.

**Определение 2.3.** *Под автоматизированной обработкой персональных данных понимается обработка с помощью средств вычислительной техники.*



При этом под средствами вычислительной техники понимаются не только стационарные компьютеры, но и все вычислительные устройства: планшеты, ноутбуки, смартфоны и другие.

Рассмотрим некоторые действия с персональными данными более подробно.

**Блокирование** персональных данных предполагает временное прекращение их обработки. После осуществления блокирования в течение определенного периода времени должно быть невозможно производить с персональными данными никаких действий. Возможность удаления, редактирования, передачи и осуществления других действий с заблокированными персональными данными должна появиться только после их разблокирования.

В отличие от блокирования, при **уничтожении** персональных данных восстановить их содержание, а также возобновить их обработку становится принципиально невозможным.

Часто действия по уничтожению ПДн подразумевают уничтожение их материальных носителей. Например, сжигание бумажного носителя или уничтожение жёсткого диска путем его расплавления.

**Обезличивание** персональных данных состоит в осуществлении действий, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту [6]. Например, пусть мы храним паспортные данные владельцев автомобилей и сведения об их транспортных средствах. Удаление паспортных данных приведет к ситуации, при которой мы не сможем соотнести транспортное средство с его владельцем.

Обратим внимание, что в приказе Роскомнадзора «Об утверждении требований и методов по обезличиванию персональных данных» [13] обезличивание персональных данных рассматривается в более широком контексте. В соответствии с этим приказом методы обезличивания делятся на обратимые и необратимые. Если после применения обратимых методов обезличивания связь между субъектом и его персональными данными можно восстановить, то после применения необратимых методов связь полностью утрачивается. Таким образом, после применения необратимых методов, полученные данные уже не являются персональными.

**Определение 2.4.** *В терминах Федерального закона «О персональных данных» оператором (персональных данных) является лицо, самостоятельно или совместно с другими лицами организующее или осуществляющее обработку персональных данных, определяющее цели обработки персональных данных и их состав, а также совершаемые с персональными данными действия.*

Таким образом, практически все организации и предприятия являются операторами (ПДн), поскольку практически каждая организация и каждое предприятие обрабатывают персональные данные хотя бы своих сотрудников.

Следует различать «оператора (ПДн)» в терминах Федерального закона «О персональных данных» и «оператора информационной системы» в терминах Федерального закона «Об информации, информационных технологиях и о защите информации». Например, пусть центр обработки данных (ЦОД) предоставляет услуги по хранению (любых) данных на серверных мощностях. Некоторые организации, пользующиеся услугами ЦОД, могут размещать на его серверных мощностях персональные данные, не уведомляя при этом ЦОД. В данной ситуации ЦОД выступает оператором своей информационной системы (инфраструктуры), но не

является оператором ПДн, поскольку не определяет цели и состав обрабатываемых данных, а также может не принимать фактического участия в их обработке.

**Определение 2.5.** *Под информационной системой персональных данных, по сути, понимается информационная система, в которой обрабатываются персональные данные.*

По составу технических средств и используемым информационным технологиям информационные системы персональных данных (ИСПДн) могут очень сильно различаться. Например, информационные системы могут состоять только из одного компьютера (автоматизированного рабочего места, АРМ) или нескольких рабочих мест, входящих в состав локальной вычислительной сети предприятия, а могут включать распределенную вычислительную инфраструктуру, охватывающую территорию субъекта Российской Федерации или всю Российскую Федерацию в целом.

Примером информационной системы, состоящей из одного АРМ, может являться компьютер врача, на котором он ведет обработку сведений о своих пациентах. Практически в каждой организации существуют кадровая и бухгалтерская информационные системы, развернутые в локальных вычислительных сетях предприятий. Информационной системой, охватывающей всю территорию Российской Федерации, является, например, Единый государственный реестр записей актов гражданского состояния (ЕГР ЗАГС).

## 2.3. Принципы обработки персональных данных

**Принцип 1** (на наш взгляд, не нуждающийся в комментариях). Обработка ПДн должна осуществляться на законной и справедливой основе [6].

**Принцип 2.** Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей [6].

Цель обработки ПДн первична. Исходя из цели, которую предстоит достигнуть, формируется состав необходимых для этого ПДн, а также устанавливаются сроки их обработки. Отметим, что не допускается обработка ПДн несовместимая с целями их сбора. Например, нельзя собирать персональные данные ветеранов Великой Отечественной войны для того, чтобы вручить им подарки к 9 Мая, и одновременно использовать эти данные для продвижения товаров и услуг или политической агитации.

**Принцип 3.** Кроме того, не допускается объединение баз ПДн, обработка которых ведется в различных, несовместимых между собой целях [6].

Например, база ПДн ветеранов Великой Отечественной войны, нуждающихся в улучшении жилищных условий, не может быть объединена с базой данных лиц, давших свое согласие на продвижение товаров и услуг, поскольку цели обработки ПДн несовместимы между собой.

**Принцип 4.** Обработке подлежат только те персональные данные, которые необходимы для достижения цели их обработки [6].

Например, для отправки почтовых сообщений достаточно хранить фамилию, имя и отчество субъекта ПДн и его почтовый адрес. Обработка паспортных данных (серия и номер паспорта, когда и кем он выдан ...) для отправки почтовых сообщений является избыточной.

**Принцип 5.** Содержание и объем обрабатываемых ПДн должны соответствовать целям обработки ПДн [6].

Существует несколько подходов к трактовке понятий «содержание» и «объем» ПДн. С одной стороны, под содержанием можно понимать актуальное состояние обрабатываемых данных, а под объемом их состав. В этом случае, если мы обрабатываем фамилии, имена, отчества, паспортные данные и сведения об образовании — это объем обрабатываемых данных. Обработка паспортных данных может быть избыточна, с точки зрения объема. Содержание же в этом случае — это конкретная обрабатываемая информация. Например, Иванов Иван Иванович, паспорт: серия 0000, номер 000000, среднее специальное образование.

С другой стороны, под содержанием можно понимать состав обрабатываемых данных, а под объемом — временной интервал, в течение которого обрабатываются персональные данные, или территориальную принадлежность субъекта ПДн. Например, если мы обрабатываем персональные данные в целях формирования налоговой отчетности за последние пять лет, то нам достаточно хранить персональные данные в «объеме» последних пяти лет. Хранение ПДн за более длительный период в данной ситуации является избыточным. Если для достижения цели обработки достаточно хранить персональные данные жителей одного из районов города Ярославля, то обработка данных всех жителей города Ярославля — избыточна. Если мы планируем проводить соревнования по бегу среди юношей от 12 до 14 лет, то у нас нет оснований для сбора информации о спортсменах-девушках и информации о спортсменах других возрастов.

**Принцип 6.** При обработке ПДн должны обеспечиваться их точность, достаточность и актуальность целям обработки [6].

Например, при выходе замуж девушки могут поменять свою фамилию на фамилию мужа. После этого они имеют право требовать у всех операторов информационных систем, в которых обрабатываются их персональные данные, актуализации информации.

**Принцип 7.** В общем случае, если для обработки ПДн отсутствуют иные законные основания, то хранение ПДн должно осуществляться только до достижения цели их обработки [6].

После достижения цели обработки ПДн, они должны быть либо обезличены, либо уничтожены, либо переведены на архивное хранение (и тем самым выведены из юрисдикции Федерального закона «О персональных данных»).

В качестве примера рассмотрим вопрос обработки ПДн сотрудников в обычных бухгалтерских и кадровых системах. В соответствии с налоговым законодательством Российской Федерации после увольнения сотрудника его персональные данные могут учитываться в налоговой отчетности в течение трех (или пяти) лет. Соответственно для обработки его ПДн в течение трех (или пяти) лет имеются законные основания (закрепленные Налоговым кодексом Российской Федерации). Если субъект не дал согласия на обработку своих ПДн в течение более длительного срока, то по достижении трех (или пяти) лет с момента увольнения сотрудника необходимо удалить его персональные данные из актуальных информационных систем. Часто сотрудники отдела кадров или сотрудники отдела бухгалтерии апеллируют к необходимости хранения ПДн уволенных сотрудников в течение 75 лет после увольнения. Однако в данном случае речь идет об архивном хранении. Как уже обсуждалось ранее, архивное хранение не предполагает хранения и обработки ПДн в актуальной информационной системе. Для перевода информации на архивное хранение мы должны записать персональные данные на отчуждаемый носитель информации, промаркировать его, переместить в «архив» (хранилище) и выдавать материалы под

роспись в соответствующем журнале. В организации должны быть разработаны и внедрены локальные нормативные акты, описывающие порядок перевода ПДн на архивное хранение. Кроме того, архивное хранение в общем случае не подразумевает возможности внесения изменений в хранимые материалы, только дополнение.

## **2.4. Основания обработки персональных данных**

Обработка ПДн допускается в следующих случаях [6]. Во-первых, субъект может дать согласие на обработку своих ПДн. Во-вторых, обработка ПДн может оказаться необходимой для достижения целей, установленных международными договорами или законодательством Российской Федерации. Далее обработка ПДн допускается, если она осуществляется в связи с участием субъектов ПДн в различных видах судопроизводства или необходима для исполнения судебного акта, акта органа государственной власти или органа местного самоуправления, а также для исполнения актов должностных лиц в случае, если эти акты подлежат исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

Обработку ПДн можно осуществлять в целях реализации Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», а также в целях исполнения договора, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения такого договора.

Обратим внимание, что согласие субъекта ПДн и договор, стороной которого является такой субъект, являются эквивалентными основаниями для осуществления обработки ПДн субъекта. Если Вы заключили с субъектом ПДн договор, в котором приводится полная и достоверная информация об обработке его ПДн, дополнительного согласия на обработку ПДн от субъекта не требуется.

Обработка ПДн допускается, если она необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, а получение согласия субъекта ПДн невозможно. Например, человек может оказаться временно недееспособным по причинам болезни или несчастного случая, при этом требуется оперативный доступ к его персональным данным для оказания медицинской помощи.

Далее обработка ПДн возможна, если она необходима для осуществления прав и законных интересов оператора ПДн или третьих лиц. В одной из последних редакций Федерального закона «О персональных данных» было непосредственно уточнено, что речь идет о защите прав кредиторов.

Кроме того, обрабатывать ПДн можно для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн, а также в рамках профессиональной деятельности журналиста, законной деятельности средства массовой информации, научной, литературной и иной творческой деятельности, в случае если при этом не нарушаются права и законные интересы субъектов ПДн.

Например, если в рамках медицинских исследований ведётся документация, в которой указываются реальные персональные данные пациентов, участвующих в исследовании, то желательно заручиться их согласием на обработку. Это связано с тем, что медицинская документация может предоставляться в различные организации (например, в медицинские институты), а также использоваться для выступлений на научных конференциях. Поскольку контролировать использование ПДн в такой ситуации достаточно трудно, то некоторые действия можно трактовать, как

нарушающие права и законные интересы субъектов ПДн несмотря на то, что такие действия могут осуществляться в рамках научной деятельности.

Обработка ПДн допускается, если она ведется в статистических или исследовательских целях или если ПДн подлежат опубликованию или раскрытию в соответствии с федеральным законодательством. Например, подлежит обязательному опубликованию информация об уровне зарплат руководителей органов государственной власти и органов местного самоуправления.

## 2.5. Согласие субъекта на обработку его персональных данных

Субъект ПДн принимает решение о предоставлении согласия на обработку своих ПДн свободно, по своей воле и в своих интересах [6]. Если субъекта заставили предоставить свои ПДн и дать согласие на их обработку, то в этом случае согласие на обработку ПДн может быть признано ничтожным.

Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. **Конкретное согласие** подразумевает отсутствие абстрактных и предельно обобщенных формулировок. Такое согласие должно быть предметным, определенным и точным. Например, конкретным сроком обработки ПДн является «пять лет после прекращения договорных отношений с работником организации», конкретной целью — «исполнение требований трудового законодательства Российской Федерации».

**Информированное согласие** подразумевает достоверность и полноту предоставляемых субъекту ПДн сведений, необходимых для принятия им решения о предоставлении согласия. Эти сведения, кроме прочего, должны содержать информацию о последствиях предоставления (или непредоставления) согласия. Например, нельзя скрывать от субъекта ПДн часть целей, для достижения которых планируется обрабатывать ПДн, или часть действий, которые будут совершаться с ПДн в процессе их обработки. Считается, что информированное согласие может дать субъект ПДн, который обладает достаточной компетентностью и дееспособностью и осознает последствия своих действий.

**Сознательное согласие** подразумевает, что субъект ПДн имеет право прочесть, понять и осмыслить предоставляемое им согласие. Кроме прочего, субъекту ПДн должно быть предоставлено необходимое для этого время.

Согласие должно включать информацию о том, в каких целях планируется обрабатывать ПДн, о перечне ПДн, необходимых для достижения целей обработки, информацию о сроках обработки ПДн, а также о действиях, которые планируется совершать с обрабатываемыми ПДн и так далее. В согласии на обработку ПДн не допускается неконкретность формулировок (размытые, абстрактные, бессодержательные формулировки) [6].

Если иное не установлено федеральным законодательством, согласие на обработку ПДн может быть дано в любой форме, позволяющей подтвердить факт его получения [6]. Например, согласие может быть дано в письменной форме или в форме электронного документа.

На настоящий момент согласия собираются также в личных кабинетах веб-сервисов в виде проставления меток в специальных формах. Обратим внимание, что законодательство Российской Федерации не предусматривает возможность подтверждения действием согласия на обработку ПДн (конклюдентного подтверждения). Например, приобретая товар в интернет-магазине, мы можем вводить в веб-формы свои персональные данные, подтверждая тем самым готовность купить

товары. Заполнение форм само по себе можно было бы рассматривать в качестве согласия на обработку ПДн. Тем не менее, по нашему законодательству согласие в такой форме не принимается и необходимо прибегать к заполнению специальных форм.

В случае, если субъект ПДн не достиг совершеннолетия или не является дееспособным, согласие на обработку его ПДн должен давать законный представитель субъекта. При этом полномочия представителя субъекта ПДн должен проверять оператор (ПДн) [6].

Субъект имеет право на отзыв согласия на обработку ПДн. В этой ситуации, если иные законные основания для продолжения обработки отсутствуют, необходимо прекратить обработку ПДн, то есть удалить их, обезличить или перевести на архивное хранение. В неправомерной обработке ПДн в первую очередь заинтересован оператор, поэтому именно на нем лежит обязанность доказывать, что субъект дал своё согласие на обработку ПДн [6].

Согласие субъекта в письменной форме должно включать [6]:

- фамилию, имя и отчество;
- адрес субъекта ПДн;
- номер основного документа, удостоверяющего личность, а также сведения о дате выдачи указанного документа и выдавшем его органе;

В силу этого требования иногда возникают парадоксальные ситуации, при которых согласие субъекта ПДн содержит больше информации, чем необходимо для достижения целей обработки.

- информацию о документах, которые подтверждают права представителя субъекта ПДн на подписание согласия от его (субъекта) имени (при необходимости);
- наименование оператора, если обработку ПДн ведёт юридическое лицо, или фамилию, имя, отчество для оператора — физического лица, а также адрес оператора;
- наименование организации или фамилию, имя, отчество физического лица, которому поручается обработка (при поручении обработки);
- цели обработки ПДн;

Цели обработки ПДн должны быть конкретными и достижимыми. Например, мы можем обрабатывать персональные данные сотрудников нашей организации в целях исполнения требований законодательства Российской Федерации (Налогового кодекса или Трудового кодекса Российской Федерации). Для достижения этих целей рассчитывается, начисляется и выплачивается заработная плата, а также рассчитываются налоги, которые должны заплатить сотрудники организации. Примерами целей обработки ПДн также будут являться оказание услуг субъекту ПДн (в том числе государственных и муниципальных) или продажа товаров.

- перечень ПДн, которые необходимы для достижения цели обработки;
- перечень действий с персональными данными, на совершение которых дается согласие и общее описание используемых оператором способов обработки ПДн.

Здесь речь идет о достаточно формальном описании действий с персональными данными, которые мы предполагаем осуществлять. Например, сбор, хранение, передача и распространение ПДн. В качестве общего описания используемых способов обработки ПДн следует указать: используются ли при обработке средства вычислительной техники, передается ли информация в сторонние организации, используется ли передача по сети Интернет и так далее. Далее у согласия должен быть определен срок действия. Например, полгода после достижения цели обработки ПДн. Запас времени может быть необходим оператору для предоставления всех необходимых видов отчетности, а также для проведения всех необходимых мероприятий по удалению, обезличиванию или переводу ПДн на архивное хранение.

Письменное согласие на обработку ПДн должно быть собственноручно подписано субъектом ПДн, дающим согласие.

Как уже говорилось ранее, в случае, если субъект ПДн является недееспособным, то согласие за него дает представитель. В случае смерти субъекта согласие на обработку его ПДн дают его наследники (в случае отсутствия согласия субъекта, полученного при его жизни). Если за субъекта ПДн согласие даёт его законный представитель, то согласие должно содержать собственноручную подпись представителя.

## **2.6. Поручение обработки персональных данных**

Оператор ПДн может поручить их обработку сторонней организации или физическому лицу. Если иное не предусмотрено федеральным законодательством, то сделать это можно только имея согласие субъекта ПДн. Поручение обработки должно быть оформлено в виде договора.

Например, для маленьких организаций может быть нецелесообразно создание своего отдела бухгалтерского учета. Поэтому они могут заказать услуги по ведению бухгалтерского учета у третьей организации. В этом случае персональные данные сотрудников маленькой организации будут обрабатываться сторонними лицами, предоставляющими услуги по ведению бухгалтерского учета. Другой пример. Компания, управляющая многоквартирными домами, может поручить расчёт стоимости жилищно-коммунальных услуг сторонней организации. Если информация, необходимая для осуществления расчетов, будет содержать персональные данные, то сторонняя организация будет осуществлять обработку ПДн по поручению компании, управляющей многоквартирными домами.

В обоих случаях необходимо заручиться согласием субъекта на поручение обработки его ПДн или предусмотреть соответствующие положения в договорах, заключаемых между организациями и субъектами ПДн. В первом случае между работодателем и его сотрудниками, а во втором — между управляющей компанией и лицами, заключившими с ней договор на обслуживание многоквартирного дома.

Организация, которой поручается обработка, обязана соблюдать принципы и правила обработки ПДн [6]. При этом обязанность по получению согласия субъекта на поручение обработки полностью лежит на организации, поручающей обработку.

В случае поручения обработки ПДн ответственность перед субъектом несет организация, поручающая обработку ПДн. Все претензии субъект будет предъявлять к ней, даже если некорректные действия с персональными данными будут совершены организацией, которой поручили обработку. Последняя в свою очередь несет

ответственность не перед субъектом ПДн, а перед организацией, поручившей ей обработку.

Если в договорах на поручение обработки ПДн не предусмотрены положения об ответственности стороны, которой поручается обработка, то привлечь ее к ответственности будет достаточно трудно. Поэтому необходимо уделять особое внимание вопросам обработки и защиты ПДн в случае поручения обработки.

Обратим внимание, что поручение обработки ПДн требуется, даже если организация, которая поручает обработку, и организация, которой поручают обработку, входят в одну группу (например, холдинг), или одна организация является подведомственным учреждением другой организации. На такое поручение будут распространяться все рассмотренные нормы федерального закона «О персональных данных».

В поручении на обработку ПДн или в договоре на поручение обработки должны быть указаны цели обработки ПДн, состав передаваемых для обработки ПДн, а также перечень действий с этими данными, которые может совершать организация-порученец [6].

Кроме того, в поручении на обработку ПДн обязательно должна быть указана ответственность организации, которой поручается обработка, а также сформулированы требования по соблюдению конфиденциальности ПДн и обеспечению их безопасности. По причинам, рассмотренным ранее, желательно указать конкретные меры по организации обработки и защиты ПДн, которые должна реализовать организация-порученец.

## **2.7. Трансграничная передача персональных данных**

В общем случае трансграничная передача ПДн, то есть передача ПДн на территорию иностранного государства, допускается в страны, обеспечивающие «адекватную» защиту прав субъектов ПДн.

В первую очередь к таким странам относятся государства, подписавшие Конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». При этом необходимо учитывать, что даже в эти страны передача ПДн может быть запрещена в целях защиты основ конституционного строя, соблюдения прав и законных интересов граждан Российской Федерации, а также обеспечения обороны и безопасности государства.

Далее, «безопасными» считаются страны, вошедшие в формируемый Роскомнадзором перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы, но обеспечивающих адекватную защиту прав субъектов ПДн.

Используя этот перечень, оператор может убедиться в том, что страна, в которую он предполагает направить персональные данные, обеспечивает достаточный уровень защиты прав субъектов ПДн.

Обратим внимание, что достаточно часто встречается следующая ситуация. Международные компании могут иметь штаб-квартиры или представительства на территории стран Евросоюза и при этом арендовать вычислительные мощности в центрах обработки данных, расположенных в совсем иных странах (например, в условном Сомали). Соответственно при передаче ПДн (например, для бронирования номеров в отелях) такой международной организации высока вероятность осуществления трансграничной передачи ПДн в Сомали.



Трансграничная передача ПДн в страны, не подписавшие Конвенцию Совета Европы и не указанные в перечне Роскомнадзора, может осуществляться только при выполнении (как минимум одного) из следующих условий [6]:

- субъект ПДн дал согласие в письменной форме на осуществление такой передачи или является стороной договора, на основании которого осуществляется передача;
- передача необходима для защиты жизни и здоровья субъекта ПДн, если получение согласия в письменной форме невозможно;
- передача осуществляется с целью реализации международных договоров Российской Федерации;
- передача необходима для защиты основ конституционного строя Российской Федерации, обеспечения обороны и безопасности государства, транспортной безопасности.

## **2.8. Особые категории персональных данных**

Выделяют три особых категории (вида) ПДн: специальные категории ПДн, биометрические ПДн и ПДн, разрешенные для распространения (ранее общедоступные ПДн), особенности обработки которых мы рассмотрим далее.

### **2.8.1. Общедоступные источники персональных данных и персональные данные, разрешенные для распространения**

Информационные ресурсы, являющиеся общедоступными источниками ПДн, могут создаваться в целях информационного обеспечения. В соответствии с [6] размещение ПДн на таких ресурсах возможно только с письменного согласия субъекта ПДн, однако на практике часто ограничиваются электронными формами получения согласия. В общедоступных источниках могут размещаться (содержаться) следующие персональные данные: фамилия, имя и отчество субъекта ПДн, дата и место рождения, адрес, сведения о профессии и иная информация, сообщаемая субъектом.

Примерами общедоступных источников ПДн являются телефонные справочники жителей городов, списки жильцов многоквартирных домов, а также открытые страницы социальных сетей ВКонтакте, Facebook и других.

При создании общедоступного источника ПДн должна быть предусмотрена возможность удаления ПДн субъекта по его требованию. Например, в социальной сети ВКонтакте предусмотрена возможность удаления личной страницы.

Обратим внимание, что после размещения своих ПДн на общедоступном ресурсе, мы предоставляем доступ к ним неограниченному кругу лиц. Эти лица могут скопировать информацию «для использования в личных целях» и, таким образом, вывести ее из-под юрисдикции Федерального закона «О персональных данных». Следовательно, копии наших ПДн, полученные из общедоступных ресурсов, могут обрабатываться сторонними лицами в течение неопределённого интервала времени.

До вступления в действие 21.03.2021 Федерального закона от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» ПДн, размещенные в общедоступных источниках, назывались «общедоступными» и составляли особый вид ПДн. Указанный федеральный закон (сохраняя положения, касающиеся общедоступных источников ПДн) вводит взамен общедоступных ПДн

новый вид ПДн — «персональные данные, разрешенные субъектом персональных данных для распространения».

**Определение 2.6.** *Персональные данные, разрешенные субъектом персональных данных для распространения, — это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.*

Разрешение на распространение ПДн дается субъектом в отдельно оформляемом согласии. При этом оператор должен предоставить субъекту возможность уточнения перечня ПДн, на распространение которых дается согласие. Например, субъект может уточнить, что дает согласие на распространение не всех контактных данных (включающих фамилию имя, отчетство, почтовый адрес, адрес электронной почты, номер сотового телефона и т.п.), а только фамилии, инициалов и адреса электронной почты. Если из согласия на обработку разрешенных для распространения ПДн явно не следует, что субъект разрешил распространение некоторых ПДн, то такие ПДн могут обрабатываться оператором (которому дается согласие) без права распространения.

Кроме того, субъект ПДн может установить в согласии обязательные для исполнения оператором запреты на передачу (кроме предоставления доступа) разрешенных для распространения ПДн оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) таких ПДн неограниченным кругом лиц. Запреты и условия, установленные субъектом ПДн, оператор обязан опубликовать (довести до сведения лиц, использующих его информационные ресурсы). В случаях обработки ПДн в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации, запреты и условия, установленные субъектом ПДн, могут не действовать.

Субъект может дать согласие оператору на обработку ПДн, разрешенных для распространения, непосредственно или с использованием информационной системы уполномоченного органа по защите прав субъектов ПДн (на момент написания учебного пособия регламент предоставления такого согласия находится на этапе разработки).

Согласие на обработку ПДн, разрешенных для распространения, действует до момента поступления оператору требования субъекта о прекращении обработки его ПДн. В таком требовании должны быть указаны фамилия, имя, отчество и контактная информация субъекта ПДн, а также перечень ПДн, обработка которых должна быть прекращена.

В случае распространения ПДн непосредственно субъектом ПДн без предоставления оператору согласия на обработку ПДн, разрешенных для распространения, и в случае распространения ПДн вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность по предоставлению доказательств законности обработки ПДн возложена на каждое лицо, осуществившее распространение или иную обработку таких ПДн.

## **2.8.2. Специальные категории персональных данных**

**Определение 2.7.** *К специальным категориям персональных данных относятся сведения, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни.*

Обратим внимание, что достаточно часто персональные данные, которые не относятся к специальным категориям, пытаются к ним отнести. Например, сведения о том, является ли субъект ПДн резидентом той или иной страны, могут пытаться рассмотреть как национальную принадлежность, или сведения о социальном статусе, например, о группе инвалидности, рассматривают как сведения о состоянии здоровья. В общем случае, гражданство не определяет национальную принадлежность субъекта ПДн, а к сведениям о состоянии здоровья рекомендуется относить информацию, определенную в соответствии с Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации» как врачебную тайну. В частности, к такой информации относятся сведения об обращении граждан за оказанием медицинской помощи, сведения о диагнозе и иные сведения, полученные при обращении лица за медицинской помощью.

Обратим внимание, что в некоторых ситуациях определить, являются ли обрабатываемые персональные данные специальными или нет, достаточно трудно. Интересным примером является обработка информации о беременности. С одной стороны, можно обратиться в этом состоянии к врачу, и врач поставит соответствующий диагноз (в соответствии с международным классификатором болезней). В такой ситуации информация о беременности будет рассматриваться как сведения о состоянии здоровья. Кроме того, сведения о беременности могут рассматриваться как информация об интимной жизни. С другой стороны, если беременность является основанием для обращения, например, в социальную службу, то ее можно рассматривать как социальную категорию (сведения о социальном положении).

В общем случае обработка специальных категорий ПДн запрещается. Исключение может быть сделано в следующих случаях [6]:

- субъект дал согласие в письменной форме на обработку специальных категорий ПДн;
  - субъект разрешил распространение своих специальных категории ПДн (при условии соблюдения оператором требований законодательства Российской Федерации);
  - для достижения целей, установленных международными договорами Российской Федерации о реадмиссии, Федеральным законом «О Всероссийской переписи населения», а также для достижения целей, установленных законодательством о государственной социальной помощи, трудовым законодательством и пенсионным законодательством Российской Федерации;
  - для защиты жизни, здоровья и иных жизненно важных интересов субъекта ПДн или других лиц, в случае если получение согласия субъекта ПДн невозможно;
- В последнем случае речь идет, например, об обработке ПДн в случае необходимости экстренного медицинского вмешательства, а субъект ПДн при этом находится в бессознательном состоянии.
- в медико-профилактических целях, а также в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка проводится лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну;

Обратим внимание на некоторые тонкие моменты, касающиеся вопросов обработки специальных категорий ПДн в медицинских учреждениях. В соответствии

с законодательством Российской Федерации «Об основах охраны здоровья граждан» обязанность соблюдать врачебную тайну возложена на медицинских и фармацевтических работников, а также на медицинскую организацию в целом. При этом под медицинским работником понимается физическое лицо, имеющее медицинское или иное образование, работающее в медицинской организации, в трудовые обязанности которого входит осуществление медицинской деятельности, или физическое лицо — индивидуальный предприниматель, который также осуществляет медицинскую деятельность. Под медицинской деятельностью понимается профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, осмотров, освидетельствований и так далее. Однако в медицинских организациях помимо медицинских работников доступ к информации о пациентах имеют, например, администраторы информационных систем и вычислительных сетей и администраторы безопасности. Поэтому в трудовых договорах с такими лицами должна быть обязательно учтена обязанность по соблюдению врачебной тайны.

- для достижения законных целей, предусмотренных учредительными документами общественных объединений или религиозных организаций, в части обработки ПДн членов (участников) таких объединений или организаций, при условии, что персональные данные не будут распространяться без согласия субъектов в письменной форме;
- для установления или осуществления права субъекта ПДн или третьих лиц, в том числе прав кредиторов, а также для осуществления правосудия;
- для реализации законодательства Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительного законодательства;
- для реализации законодательства Российской Федерации об обязательных видах страхования и страхового законодательства;
- в целях устройства детей, оставшихся без попечения родителей, на воспитание;
- для реализации законодательства о гражданстве Российской Федерации.

### **2.8.3. Биометрические персональные данные**

В соответствии с Федеральным законом «О персональных данных» под биометрическими ПДн понимаются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность. При этом особые правила обработки биометрических ПДн (по отношению к иным ПДн) предусматриваются Федеральным законом «О персональных данных» только для тех случаев, при которых оператор непосредственно использует эти данные для установления личности. Обработка биометрических ПДн, которые не используются для установления личности субъекта, осуществляется на общих основаниях.

Рассмотрим пример. Прямое назначение фотографии в паспорте — идентификация человека. Поэтому фотография в паспорте относится к биометрическим ПДн, используемым для установления личности. Однако та же самая фотография, находящаяся, например, в памятном альбоме, не предполагает использования

для установления личности и поэтому особые правила обработки биометрических ПДн, установленные Федеральным законом «О персональных данных», на нее не распространяются.

Примерами биометрических ПДн являются:

- фотография, выполненная при определенных условиях (например, фотография в паспорте);
- отпечатки пальцев или отпечатки папиллярных узоров других частей тела;
- рисунок кисти руки;
- рисунок капиллярных узоров лиц;
- рисунок сетчатки глаза;
- написанный от руки достаточно длинный текст;
- достаточно длинное голосовое сообщение.

На обработку биометрических ПДн, используемых оператором для установления личности, требуется получить письменное согласие субъекта ПДн. Без согласия такие ПДн могут обрабатываться в случаях, если это необходимо для реализации международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия или исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне и безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством, законодательством о порядке выезда из Российской Федерации и въезда в Российскую Федерацию и о гражданстве Российской Федерации [6].

## **2.9. Права субъекта персональных данных**

Субъект имеет право запрашивать и получать у оператора информацию, касающуюся обработки его ПДн [6]. Эта информация во многом совпадает с той, которую оператор должен предоставить субъекту при взимании с него согласия на обработку, поэтому мы не будем акцентировать на ней внимание.

Отметим только, что субъект имеет право на получение сведений о лицах, имеющих доступ к персональным данным, и лицах, которым персональные данные могут быть раскрыты по договору или на основании федерального законодательства. Важно понимать, что в этой ситуации речь идет о юридических лицах, с которыми взаимодействует оператор, а не о физических лицах, например, сотрудниках оператора, осуществляющих обработку ПДн.

Рассмотрим следующий пример. Пусть субъект ПДн покупает путевку у туроператора. Туроператор использует предоставленные субъектом персональные данные для заключения договоров с гостиницами и автотранспортными компаниями. В этом случае субъект имеет право получить информацию о том, каким гостиницам и автотранспортным компаниям передаются его персональные данные.

Кроме того, субъекту должна быть предоставлена информация о порядке осуществления им всех своих прав. В частности, должен быть предложен конкретный

алгоритм действий в случае, если субъект обнаружит факт обработки избыточных, неактуальных или незаконно полученных ПДн.

Запрашиваемая информация должна быть предоставлена субъекту ПДн в доступной для него форме.

Права субъекта на доступ к его персональным данным могут быть ограничены в ситуациях, в основном связанных с обеспечением безопасности и правопорядка, а именно, права субъекта могут быть ограничены, если обработка ПДн осуществляется [6]:

- правоохранными органами, осуществившими задержание субъекта ПДн, либо предъявившими ему обвинение по уголовному делу, либо применившими к субъекту меру пресечения до предъявления обвинения;
- в целях обеспечения обороны страны, безопасности государства и охраны правопорядка;
- в соответствии с законодательством о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма;
- в соответствии с законодательством о транспортной безопасности.

Особенной является ситуация, при которой доступ субъекта к его персональным данным может быть ограничен, поскольку нарушает права и законные интересы третьих лиц. В этом случае речь идет скорее о формате представления информации. К примеру, наша информационная система может не позволять выводить на печать информацию только об одном субъекте ПДн и всегда выдает на печать информацию о нескольких субъектах. Получив распечатанные данные о субъекте, мы не можем передать их ему вместе с персональными данными третьих лиц. При этом мы можем после печати «вырезать» персональные данные субъекта, запросившего информацию и передать их ему уже без ПДн посторонних лиц.

Если субъект обнаруживает, что оператор обрабатывает его персональные данные, которые не являются актуальными (неполными, устаревшими, неточными) или являются избыточными по отношению к целям обработки или незаконно полученными, то субъект ПДн имеет право требовать от оператора уточнения, блокирования или уничтожения таких ПДн [6].

Например, пусть социальная служба обрабатывает информацию о семье, в которой есть двое детей. Спустя какое-то время в семье может появиться третий ребёнок, но социальная служба продолжит обрабатывать информацию только о двух детях. В этом случае один из родителей имеет право требовать уточнения неполной информации.

Субъект ПДн имеет право обратиться в Роскомнадзор или суд с целью обжаловать действия или бездействие оператора, если считает, что оператор нарушает требования Федерального закона «О персональных данных». Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда, решение о которых принимается в судебном порядке [6].

**Права субъекта при обработке его ПДн в целях продвижения товаров, работ и услуг на рынке, а также в целях политической агитации.**

Обработка ПДн в целях продвижения товаров, работ и услуг на рынке с помощью прямых контактов с потенциальными потребителями с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта ПДн [6].

Под прямым контактом здесь понимается «персонифицированный» контакт. Например, Вам звонят по телефону и обращаются по имени и отчеству, либо вам приходит (бумажное или электронное) письмо с личным обращением. Не относятся к прямым контактам массовая рассылка однотипных сообщений или телефонные звонки, осуществляемые на основе случайного выбора номера телефона без личного обращения.

Интересным примером в данном случае является печать рекламы на счетах за коммунальные услуги. Поскольку на счетах за жилищно-коммунальные услуги указываются фамилии и инициалы субъектов ПДн, а также адреса, то можно считать, что в данном случае реклама осуществляется с помощью прямых контактов с потенциальным потребителем. Возможность такой интерпретации породила достаточно большое число обращений граждан в Роскомнадзор и прокуратуру. Однако на судебных разбирательствах управляющим компаниям удалось показать, что сначала они печатали на листах бумаги, предназначенных для печати счёта, рекламу, и только после этого печатали на этих листах счета. Таким образом, персональные данные появлялись на листах с уже напечатанной рекламой, то есть реклама не имела персонифицированной направленности и предназначалась для неопределенного круга лиц. Отметим, что конвертование счетов за коммунальные услуги также связано с обеспечением безопасности ПДн.

**Права субъекта при принятии юридически значимых для него решений на основании исключительно автоматизированной обработки его персональных данных.**

Вначале обратим внимание, что исключительно автоматизированная обработка ПДн исключает возможность влияния человека на результаты обработки. Многие процессы, которые представляются нам полностью автоматизированными, на самом деле предполагают наличие оператора или эксперта, который принимает окончательное решение на основании полученной с помощью средств вычислительной техники информации.

В частности, при нарушении автомобилем скоростного режима, фиксация нарушения осуществляется с помощью камер видеонаблюдения. Полученные при этом снимки направляются оператору информационной системы (в Центр автоматизированной фиксации административных правонарушений в области дорожного движения ГИБДД, ЦАФАП), который принимает решение о том, было ли совершено нарушение, и можно ли однозначно идентифицировать автомобиль на снимке. Если оба решения положительные, то оператор направляет информацию в ГИБДД и уже на основании этой обработанной и проверенной информации владельцу автомобиля назначается штраф.

Другой пример. Сведения о состоянии здоровья могут быть получены с помощью исключительно автоматизированной обработки на медицинском оборудовании, но интерпретирует эту информацию и назначает лечение врач.

Примеров исключительно автоматизированной обработки ПДн существенно меньше. Такая обработка может осуществляться при тестировании школьников с помощью компьютеров, при этом обработка информации, включая выставление оценки учащемуся, должна полностью осуществляться компьютером (без привлечения педагога). В частности, в наших курсах результаты тестирования будут определяться на основании исключительно автоматизированной обработки.

В общем случае, принятие юридически значимых решений для субъекта на основании исключительно автоматизированной обработки его ПДн запрещается [6].

Исключениями являются случаи, при которых субъект дал на это свое согласие в письменной форме, или принятие юридически значимых решений на основании исключительно автоматизированной обработки предусматривается федеральными законами, которые, кроме прочего, должны определять порядок соблюдения обеспечения прав и законных интересов субъектов ПДн.

При принятии юридически значимых решений на основании исключительно автоматизированной обработки ПДн, оператор обязан разъяснить субъекту ПДн порядок принятия решений, а также возможные юридические последствия. Кроме того, оператор обязан предусмотреть возможность несогласия субъекта с принятым решением, разъяснить ему порядок защиты своих прав и законных интересов, а также организовать работу с возражениями субъектов [6].

## **2.10. Меры обеспечения безопасности персональных данных**

Оператор обязан принимать необходимые и достаточные меры для выполнения требований Федерального закона «О персональных данных» и подзаконных актов, состав которых он вправе определять самостоятельно. Однако поскольку существующая нормативно-правовая база, регламентирующая вопросы организации обработки и защиты ПДн, достаточно широка, то, фактически, оператор вправе выбирать не состав мер, а конкретные решения для их реализации.

Следует отметить, что во многих случаях требования Федерального закона «О персональных данных» и подзаконных актов являются требованиями достаточно высокого уровня. Например, существуют требования по разработке определенной документации. Однако нет требований к содержанию данной документации. Это оставляет возможность для творчества оператора.

Перейдем к рассмотрению состава мер, определенного Федеральным законом «О персональных данных». В первую очередь, в организации-операторе должно быть назначено лицо, ответственное за организацию обработки ПДн [6]. В качестве ответственного лица рекомендуется назначать одного из заместителей руководителя организации-оператора. Считается, что при таком подходе ответственное лицо сможет скоординировать работы по организации обработки и защиты ПДн в рамках всей организации.

Далее, оператор должен принять политику в отношении обработки ПДн, а также ряд локальных нормативных актов, регулирующих вопросы обработки ПДн в организации-операторе [6].

Оператор обязан обеспечить неограниченный доступ лиц к политике обработки ПДн. Причём он должен это сделать с использованием технологий, используемых для сбора ПДн. К примеру, если оператор собирает информацию на бумажных носителях в своем офисе, то в этом случае он должен поместить политику обработки ПДн на стенды, чтобы каждый проходящий в офис смог с ней ознакомиться. Если же оператор осуществляет сбор ПДн с использованием сети Интернет, то он должен опубликовать свою политику в этой сети.

Отметим, что помимо правовых и организационных мер оператор должен реализовать и технические меры защиты ПДн [6].

Кроме принятия первоочередных мер по организации обработки и защиты ПДн, оператор должен организовать проведение внутреннего контроля и аудита соответствия обработки ПДн требованиям Федерального закона «О персональных данных» и подзаконных актов [6].



Особое место при проведении внутреннего контроля должна занимать проверка актуальности принятых мер действующим нормам законодательства. Это связано в первую очередь с тем, что законодательство в сфере обработки ПДн является достаточно динамичным. Поэтому мероприятия, которые были актуальны некоторое время назад, могут оказаться неактуальными к моменту контроля. Кроме того, достаточно часто происходит изменение в технологических процессах обработки ПДн, после чего должны изменяться принятые меры. Однако на практике этого зачастую не происходит. Например, в организации-операторе увольняется сотрудник, ответственный за организацию обработки ПДн. После этого должен быть назначен другой ответственный, но этого не происходит.

Также следует внимательно отнестись к вопросам изменения правовых оснований обработки ПДн. Часто возникают ситуации, при которых ранее обработка ПДн предписывалась правовыми актами, но с прошествием времени эти акты были либо отменены, либо изменены. При этом обработка продолжает осуществляться по прежним правилам. Таким образом, технологические процессы обработки ПДн перестают соответствовать действующему законодательству Российской Федерации и теряют свою легитимность. В настоящий момент такая ситуация может произойти при применении органами государственной власти регуляторной гильотины.

Далее, оператор должен производить оценку вреда, который может быть причинен субъектам ПДн. В настоящий момент эта оценка осуществляется в рамках моделирования нарушителей и угроз безопасности ПДн, о которой будем говорить в следующей теме [6].

Кроме того, оператор должен обеспечить ознакомление своих сотрудников, осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями по их защите, а также локальными нормативными актами оператора, регулирующими обработку ПДн, провести обучение сотрудников по этим вопросам [6].

В состав технических мер по обеспечению безопасности ПДн входят следующие мероприятия [6]:

- определение актуальных угроз безопасности ПДн (организационная мера, результатом которой является разработанная модель нарушителей и угроз безопасности ПДн);
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (то есть сертифицированных средств защиты информации);
- оценка эффективности применяемых мер по обеспечению безопасности (организационная мера, которую можно реализовать в различных формах. На настоящий момент, наиболее распространенная форма — аттестация информационной системы);
- учет машинных носителей ПДн (организационная мера, предполагающая поштучную перепись всех носителей ПДн и организацию их оборота);
- обеспечение безопасности ПДн от несанкционированного доступа, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них (организационно-техническая мера, может

быть реализована с помощью различных средств защиты информации, например, систем обнаружения вторжений, антивирусных средств, средств предотвращения утечек, SIEM-систем и т. д., при этом подразумевает наличие подразделения по информационной безопасности или договора на обслуживание со сторонней организацией – лицензиатом ФСБ России и ФСТЭК России, поскольку требует достаточно высокого уровня компетенций у реализующих ее лиц);

- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа (техническая мера, которую можно реализовать с помощью средств резервного копирования и восстановления после сбоя);
- разграничение прав доступа к персональным данным (можно реализовать с помощью организационных мер, а также с помощью применения средств защиты от несанкционированного доступа);
- регистрация и учет всех действий с персональными данными (техническая мера, которую можно реализовать с помощью систем регистрации и учета или аудита событий);
- контроль за принимаемыми мерами (организационная мера, которая использует материалы, полученные с помощью средств защиты информации в качестве входных данных).

## **2.11. Контроль и надзор за выполнением мер по обеспечению безопасности**

Регуляторами, осуществляющими контроль и надзор в сфере обработки и защиты ПДн, являются Роскомнадзор, Федеральная служба безопасности Российской Федерации (ФСБ России) и Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России).

Роскомнадзор является федеральным органом государственной власти, уполномоченным на защиту прав субъектов ПДн. Именно Роскомнадзор осуществляет основные проверки по тематике соблюдения требований законодательства о ПДн. Его сфера проверок — это правовая часть исполнения требований Федерального закона «О персональных данных» и подзаконных актов. Это единственный из регулирующих органов, который имеет право получать доступ к обрабатываемым персональным данным с целью обнаружения фактов нарушения законодательства.

Кроме проведения проверок, Роскомнадзор организует защиту прав субъектов ПДн, рассматривает жалобы и обращения по вопросам, связанным с обработкой ПДн, а также принимает решения по результатам рассмотрения указанных жалоб и обращений [6]. Например, он может обязать оператора изменить состав обрабатываемых ПДн или прекратить их обработку.

ФСБ России и ФСТЭК России осуществляют контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности ПДн, которые либо обрабатываются в государственных информационных системах, либо представляют чрезвычайную важность (достаточную для того, чтобы наделять ФСТЭК России и ФСБ России полномочиями по их индивидуальному контролю).

Де-юре ФСБ России должна контролировать процессы применения криптографических средств защиты информации для защиты ПДн, а ФСТЭК

России — процессы применения иных технических средств защиты. Однако фактически организационная структура ФСТЭК России включает только управления по Федеральным округам, что ограничивает ее возможности по проведению проверок, поэтому часть ее контролирующих функций переданы ФСБ России. Управления ФСБ России в субъектах Российской Федерации осуществляют контроль исполнения требований обеих служб по технической защите ПДн. При проведении проверок ФСБ России и ФСТЭК России не имеют права знакомиться с персональными данными (то есть получать к ним доступ).

## **2.12. Вопросы и задания**

**2.1.** Дайте определение понятию «персональные данные».

**2.2.** На какие отношения не распространяется действие федерального закона «О персональных данных»?

**2.3.** Какие отношения регулирует федеральный закон «О персональных данных»?

**2.4.** Дайте определения понятиям «обработка», «обезличивание», «блокирование» и «уничтожение» персональных данных.

**2.5.** Чем отличаются оператор информационной системы и оператор в определении федерального закона «О персональных данных»?

**2.6.** Выберите верные утверждения. Обработка персональных данных:

1. Должна ограничиваться достижением конкретных, заранее определенных и законных целей.
2. Не допускается без согласия субъекта персональных данных.
3. Не допускается в случаях, несовместимых с целями сбора персональных данных.
4. Должна осуществляться на законной и справедливой основе.

**2.7.** В каких случаях допускается обработка персональных данных?

**2.8.** Кто несет ответственность за действия юридического лица, которому поручена обработка персональных данных, перед субъектом персональных данных?

**2.9.** Какие сведения должны обязательно содержаться в поручении на обработку персональных данных?

**2.10.** На ком лежит обязанность по доказательству получения согласия от субъекта персональных данных?

**2.11.** Какие сведения должно включать согласие субъекта на обработку его персональных данных?

**2.12.** Кто должен давать согласие на обработку персональных данных в случае смерти субъекта персональных данных?

**2.13.** Какие сведения относятся к специальным категориям персональных данных?

**2.14.** Какие сведения с точки зрения Федерального закона «О персональных данных» относятся к биометрическим персональным данным?

**2.15.** Кто обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных?

**2.16.** На получение какой информации, касающейся обработки его персональных данных, имеет право субъект персональных данных?

**2.17.** В каких случаях право гражданина на получение информации, касающейся обработки его персональных данных, может быть ограничено?

**2.18.** Какие органы государственной власти осуществляют контроль и надзор за выполнением мер по обеспечению безопасности персональных данных? Каковы их области контроля и надзора?

### 3. Организационные основы обеспечения информационной безопасности

#### 3.1. Организационные основы обеспечения информационной безопасности. Алгоритм действий

Общий подход к обеспечению безопасности (не только информационной) состоит в последовательном получении ответов на следующие вопросы.

1. Что нам дорого? Что мы не хотим потерять?

Ответ на этот вопрос позволяет определить объект защиты. В общем случае, объектом защиты может быть человек (например, друг, родственник), предмет (например, кошелек, кредитная карта, машина), здание или сооружение (например, дом, мост), информация (например, данные банковского счета, медицинские данные). С точки зрения информационной безопасности основным объектом защиты выступает информация, а также ее носители (не только бумажные и, например, жесткие диски, но и физические поля, а также, люди). Обратим внимание, что необходимость защиты физических полей отнюдь не является экзотикой, например, широко распространенные бесконтактные платежные карты требуют обеспечения безопасности при передаче информации с помощью электромагнитного поля.

2. Кто наш «враг»? Кого (или чего) мы боимся? Какими ресурсами он обладает? Как он будет действовать?

Ответ на этот вопрос определяет круг лиц, заинтересованных в действиях с объектом защиты, которые мы, по каким-либо причинам, хотим ограничить или принципиально не допустить. Например, мы не хотим предоставлять данные нашего банковского счета посторонним лицам, но понимаем, что некоторые из них заинтересованы в получении таких данных для использования в целях личного обогащения.

В области информационной безопасности «врага» принято называть злоумышленником (обычно для внешних субъектов, целенаправленно идущих на нарушение закона, злонамеренное действие) или нарушителем (обычно в отношении лиц, знающих установленные правила, но осознанно или неосознанно их нарушающих). Мы будем придерживаться термина «нарушитель».

3. Какие у нас есть особенности, слабости? Как их можно использовать против нас?

Наши слабости — это возможности для нарушителей. Если мы не осознаем наши слабости, то не понимаем, как на нас могут напасть, и не можем выработать решения по противодействию. Например, мы обрабатываем данные о своем банковском счете на персональном компьютере и смартфоне. Следовательно, получив доступ к этим устройствам, нарушитель сможет получить информацию о нашем банковском счете.

4. Как мы будем защищаться? С помощью каких средств? Какими методами?

Зная свои слабости, мы можем разработать план защиты. В плане защиты мы должны определить, какими методами и средствами мы будем защищаться. План

должен предусматривать создание дополнительных барьеров для нарушителя при попытке использования им любой нашей слабости. Например, понимая, что хранение на персональном компьютере пароля для приложения клиент-банк может привести к получению доступа к нему со стороны нарушителя, необходимо определить: будем ли мы использовать для противодействия средства антивирусной защиты или будем шифровать пароль с помощью криптографических средств, или вовсе откажемся от хранения пароля на персональном компьютере.

5. Имеется ли у нас все необходимое для защиты?

Если в соответствии с планом защиты нам не хватает каких-либо навыков или средств защиты, мы должны их приобрести и использовать, в частности, установить и настроить средства защиты информации (например, средство антивирусной защиты). После того как все необходимое в соответствии с планом будет реализовано, можно говорить о создании системы защиты.

6. Готовы ли мы отразить «атаку»?

После того как создание системы защиты завершено, необходимо проверить, действительно ли она работает. Возможно, мы что-то не учли или допустили неточности при ее создании. Если при проверке будут обнаружены изъяны в системе защиты, то следует вернуться к ответу на первый вопрос и повторить все дальнейшие действия. Если проверка покажет, что система защиты работоспособна и обеспечивает требуемый уровень безопасности, то можно переходить к этапу эксплуатации системы защиты.

В сфере защиты информации последовательность ответов на приведенные выше вопросы сформировала следующую этапность проведения работ и оказания услуг.

Таблица 2.  
Этапы проведения работ и оказания услуг по защите информации

№	Наименование этапа	На какой вопрос призван ответить этап	Подэтапы	Актуальность для применения в домашних условиях
1	Выявление и анализ информационных активов	Что нам дорого? Что мы не хотим потерять?		Актуально. Необходимо определить, какая информация представляет для Вас ценность

№	Наименование этапа	На какой вопрос призван ответить этап	Подэтапы	Актуальность для применения в домашних условиях
2	Формирование требований к защите информации	Кто наш «враг»? Кого (или чего) мы боимся? Какими ресурсами он обладает? Как он будет действовать?	Моделирование нарушителей и угроз информационной безопасности. Категорирование (классификация) информации	Актуально. Необходимо понять, от кого Вы будете защищать информацию. Это не обязательно должны быть посторонние лица, например, если Вы работаете дома, то обеспечение целостности информации в рабочих документах, при условии игр Ваших детей на рабочем компьютере может являться актуальной задачей
3	Проектирование (разработка) системы защиты информации	Как мы будем защищаться? С помощью каких средств? Какими методами?		Можно ограничиться принципиальным решением о применении тех или иных средств защиты информации, но правила их настройки лучше сформулировать формально и убедиться, что они позволяют реализовать требующиеся Вам функции

№	Наименование этапа	На какой вопрос призван ответить этап	Подэтапы	Актуальность для применения в домашних условиях
4	Создание системы защиты информации	Имеется ли у нас все необходимое для защиты?	Закупка, установка и настройка средств защиты информации. Внедрение системы защиты информации (организационные мероприятия). Разработка организационной и эксплуатационной документации	Можно ограничиться покупкой, установкой и настройкой средств защиты информации
5	Оценка соответствия объекта информатизации	Готовы ли мы отразить «атаку»?	Анализ защищенности. Тестирование на проникновение. Аттестация	Можно ограничиться контролем работоспособности средств защиты информации
6	Эксплуатация системы защиты информации	Этап подразумевает периодическое повторение ответов на все вопросы в соответствии с приведенным порядком		Актуально. На этом этапе необходимо регулярно контролировать работоспособность средств защиты информации, а также периодически проверять, является ли актуальной созданная система защиты. Например, через некоторое время могут появиться новые объекты защиты, которые не были учтены при создании системы защиты и ее будет необходимо актуализировать (донастроить или дополнить)



## 3.2. Выявление и анализ информационных активов

Итак, при начале работ по защите информации в первую очередь мы должны выявить информационные активы. Основным активом будет являться та информация, которая представляет для нас ценность и которую мы хотим защищать. Зафиксировав такую информацию, мы сможем установить места её хранения и обработки, а также выявить каналы связи, используемые при передаче информации. Это позволит нам определить информационные системы, в которых обрабатывается защищаемая информация.

Традиционно выделяют два подхода к выявлению информационных активов. Первый подход основывается на анализе вычислительной инфраструктуры организации. Он предполагает исследование серверов, автоматизированных рабочих мест, коммутационного оборудования и описания информации обрабатываемой на каждом средстве вычислительной техники, а также информационных потоков в вычислительной инфраструктуре.

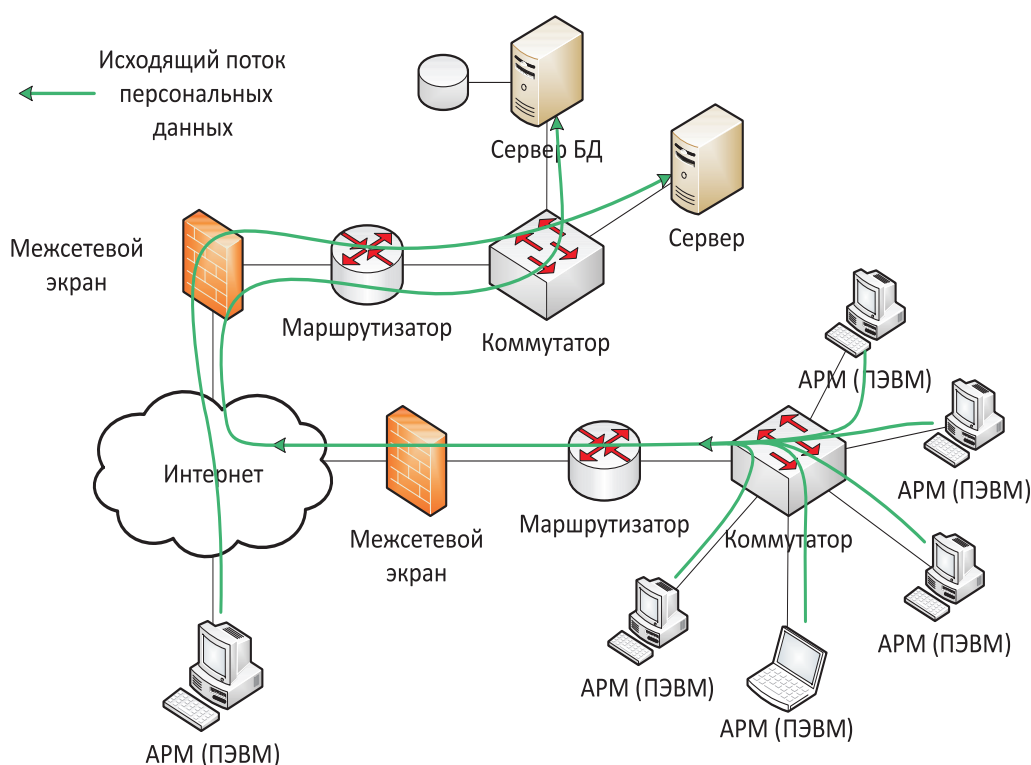


Рис. 1. Схема распределенной вычислительной инфраструктуры

На рисунке 1 представлена схема распределенной вычислительной инфраструктуры, которую можно получить с помощью первого метода. Будем считать, что в данном случае на всех указанных на схеме автоматизированных рабочих местах и серверах ведется обработка персональных данных.

Альтернативный подход базируется на анализе организационно-штатной структуры организации. При этом подходе путем интервьюирования представителей подразделений организации должны быть получены ответы на следующие вопросы:

1. Какая информация обрабатывается в подразделении?

2. Какова значимость этой информации для подразделения?
3. Какие средства вычислительной техники участвуют в обработке информации?
4. Какие информационные технологии применяются при обработке информации?
5. Каким подразделениям или сторонним организациям передается информация в процессе обработки?

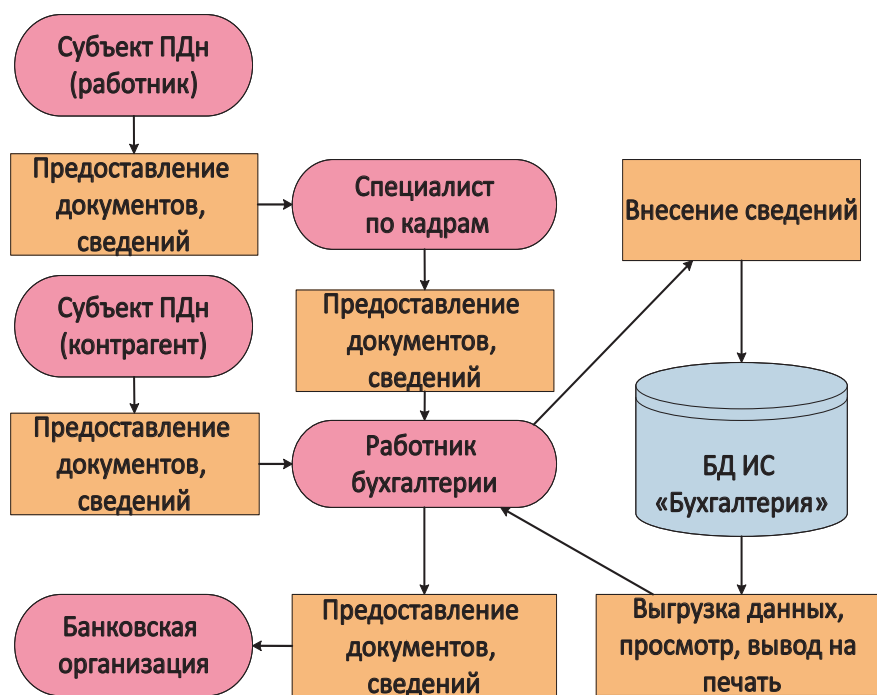


Рис. 2. Схема информационных потоков отдела бухгалтерского учета

На рисунке 2 приведена схема информационных потоков отдела бухгалтерского учета, которую можно получить с помощью второго подхода. Входящими для отдела бухгалтерского учета являются потоки, которые исходят от отдела кадров и непосредственно от субъектов персональных данных, являющихся сторонами договоров. Исходящим потоком является поток в банковскую организацию.

Кроме этого, сотрудники бухгалтерии непосредственно осуществляют обработку защищаемой информации в базе данных информационной системы «Бухгалтерия», в том числе вносят и выгружают данные.

Для достижения наиболее достоверных результатов необходимо комбинировать оба описанных подхода и использовать информацию, полученную в рамках одного подхода, для проверки информации, полученной в рамках другого подхода.

О некоторых нюансах выявления информационных активов Вы можете узнать, изучив дополнительные материалы.

Результатом выявления и анализа информационных активов будут являться:

1. Перечень сведений, которые мы планируем защищать (защищаемая информация, например, персональные данные или коммерческая тайна).

2. Характеристики безопасности информации, которые мы должны обеспечить (то есть собственно то, от чего мы хотим защищать информацию, в первом приближении: конфиденциальность, целостность и доступность).
3. Сведения о применяемых технологиях обработки информации.
4. Сведения о средствах вычислительной техники, на которых осуществляется обработка защищаемой информации.
5. Перечень информационных систем, в которых обрабатывается защищаемая информация.
6. Сведения об используемых каналах связи.
7. Сведения об используемых съемных носителях.
8. Сведения о взаимодействующих системах.
9. Сведения о применяемых методах и используемых средствах защиты информации (правовых, организационных, технических).
10. Перечисленные выше сведения в совокупности формируют модель защищаемой информационной инфраструктуры.

В качестве примера рассмотрим модель «домашней» информационной инфраструктуры. Защищаемая информация в этом случае может представлять собой Ваши личные фотографии, сканированные копии документов, служебные сведения (если Вы работаете с домашнего компьютера). В ее отношении Вы можете предъявлять требования по обеспечению конфиденциальности, целостности или доступности.

Домашняя информационная система может включать один или несколько компьютеров и смартфонов, имеющих доступ к сети Интернет посредством домашнего Wi-Fi-роутера, или состоять из одного компьютера, подключенного к сети Интернет с помощью «витой пары». Вспомогательными техническими средствами могут выступать сканеры, принтеры и другие технические средства, не применяемые для обработки защищаемой информации. На указанных технических средствах могут быть установлены операционные системы семейств Windows (например, Windows 7 или Windows 10) или Linux (например, Ubuntu, Android и другие). При обработке информации могут применяться офисные пакеты программ, программное обеспечение для обработки фотографий, видео и т. п. В качестве съемных носителей могут использоваться flash-накопители и портативные жесткие диски. Средствами защиты информации могут выступать встроенные в операционные системы сетевые экраны (например, сетевой экран Windows или IP Tables для Linux, а также антивирусное программное обеспечение (например, Dr. Web, Касперский, Avast, NOD 32). Ваши информационные системы могут взаимодействовать с автоматизированными банковскими системами, Порталом государственных услуг, Единой государственной системой в сфере здравоохранения.

### **3.3. Моделирование нарушителей и угроз информационной безопасности**

После того как мы определили перечень информационных активов, характеристики безопасности информации, которые требуется обеспечить, а также описали схему

вычислительной инфраструктуры и схему информационных потоков, мы должны перейти к формированию требований по защите информации. Требования по защите информации произрастают из двух принципиально разных источников. Первый из них — это модель нарушителя и угроз информационной безопасности. Неформально это документ, который отвечает на два вопроса: «Кто для нас является «врагом»?» (то есть кому интересно осуществить несанкционированные действия с нашей информацией, какими ресурсами и какой мотивацией он обладает), «Как на нас будут нападать?» (то есть какие у нас есть слабые места и какие действия может предпринять «враг» для того, чтобы их использовать). Второй — акт категорирования (классификации) информации (информационной системы), определяющий важность (критичность) информации (информационной системы) по сравнению с другими системами.

### 3.3.1. Моделирование нарушителей

Процесс ответа на вопрос «Кто для нас является «врагом»?» носит название моделирование нарушителя.

**Определение 3.1.** *Нарушитель безопасности информации — это физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации.*

Основной задачей моделирования нарушителя является не только определение круга лиц, заинтересованных в несанкционированных действиях с защищаемой информацией, но и оценка их возможностей: доступных ресурсов (в том числе навыков, материальных и технических средств), а также мотивации (неотступности в своем желании). Так может оказаться, что нарушитель имеет очень большое желание осуществить определенное действие, но не имеет технической возможности. С другой стороны, возможно, что нарушитель обладает техническими возможностями, но совершение действия для него не является принципиально необходимым.

Простейшая классификация нарушителей связана с понятием контролируемой зоны.

**Определение 3.2.** *Контролируемая зона — это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств.*

Например, в крупных офисных центрах доступ посетителей без предъявления паспорта возможен только на ограниченную территорию (обычно холл или фойе). Для прохода на остальную территорию здания необходимо вызвать (для сопровождения) представителя организации, в которую Вы пришли, а также предъявить паспорт и получить пропуск на территорию у вахтовой службы (или в отделе пропусков). Эта территория и будет являться контролируемой зоной (в описанной ситуации).

По наличию права постоянного или разового доступа в контролируемую зону организации нарушители делятся на внешних, не имеющих прав доступа и реализующих угрозы из внешних (неконтролируемых) сетей связи (например, Интернет), и внутренних, имеющих доступ и реализующих угрозы непосредственно в пределах контролируемой зоны.

Примерами внешних нарушителей являются [15]:

- разведывательные службы государств (большинство граждан, не связанных с управлением государством или крупными организациями, не представляют для них непосредственного интереса);

- криминальные структуры (наибольший интерес для них представляют финансовые и материальные активы граждан);
- конкуренты (например, конкуренты за должность или положение в компании потенциально могут пытаться получить доступ к Вашему рабочему компьютеру, в том числе при его домашнем использовании);
- недобросовестные партнеры (в том числе поставщики программного обеспечения и технических средств, например, при приобретении программного обеспечения на непроверенных сайтах);
- внешние субъекты (физические лица, обычно осуществляющие действия из любопытства или для «отрицательного» самоутверждения).

По определению внешний нарушитель не может находиться внутри контролируемой зоны. Поэтому его возможности по доступу к информационной инфраструктуре ограничены. Однако внешний нарушитель имеет доступ [15]:

- к каналам связи, выходящим за пределы контролируемой зоны (в том числе к каналам сети Интернет);
- к автоматизированным рабочим местам, подключенным к неконтролируемым сетям связи (например, сети Интернет);
- к элементам информационной инфраструктуры, которые оказываются за пределами контролируемой зоны (например, к переносным средствам вычислительной техники: ноутбуку, планшету или смартфону или техническим средствам, функциональное назначение которых предполагает размещение вне пределов контролируемой зоны: банкоматам, инфоматам и т. п.).

При этом возможный инструментарий внешнего нарушителя достаточно широк. Потенциально он может [15]:

- встраивать аппаратные закладки в технические средства, находящиеся за пределами контролируемой зоны;
- создавать программные закладки в программном обеспечении или данных, поступающих в Вашу локальную сеть посредством сети Интернет;
- применять вредоносное программное обеспечение;
- осуществлять атаки на элементы информационной инфраструктуры, доступные из неконтролируемых сетей связи (например, сети Интернет);
- использовать информационные системы, взаимодействующие с Вашими информационными системами, в качестве промежуточного звена в атаке.

Внутренних нарушителей можно разделить на две большие группы в зависимости от уровня их полномочий и возможностей. Первую группу формируют лица, являющиеся пользователями информационной инфраструктуры, но не обладающие существенными привилегиями, а также лица имеющие права доступа в помещения, но не имеющие прав доступа к техническим средствам информационной инфраструктуры (например, обслуживающий персонал: уборщицы, сантехники, электрики или посетители).

Вторую группу формируют лица, обладающие более высоким уровнем привилегий, а также обычно более высоким уровнем компетенций в отношении информационной инфраструктуры. В эту группу могут входить [15]:

- пользователи информационной системы с полномочиями администратора безопасности;
- пользователи информационной системы с полномочиями системного администратора информационной системы;
- программисты-разработчики прикладного программного обеспечения;
- лица, обеспечивающие сопровождение прикладного программного обеспечения (например, представители разработчика программного обеспечения);
- лица, обеспечивающие, сопровождение и ремонт технических средств.

Возможности представителей второй группы очень велики. В качестве примера, достаточно сказать, что администратор безопасности практически всегда имеет возможность отключения средств защиты информации, а системный администратор может выдать себя за практически любого пользователя информационной системы. Поэтому при приеме сотрудников на должности, предполагающие привилегированный доступ к информационной инфраструктуре, необходимо осуществлять тщательный отбор претендентов. Руководствоваться при этом необходимо не только оценкой уровня знаний, умений и навыков потенциального сотрудника (это тоже крайне важно!), но и его морально-этическими характеристиками. Кроме того, необходимо создавать условия (и поощрять их создание) для осуществления взаимного контроля представителей второй группы.

Инструментарий внутренних нарушителей включает в себя инструментарий внешних нарушителей. Кроме того, внутренний нарушитель может [15]:

- встраивать аппаратные закладки в технические средства, находящиеся в контролируемой зоне;
- создавать программные закладки в программном обеспечении или данных, циркулирующих внутри локальной вычислительной сети;
- осуществлять атаки на элементы информационной инфраструктуры, изнутри локальной вычислительной сети;
- использовать штатные возможности программного обеспечения информационных систем, к которым он имеет доступ.

Для домашней информационной инфраструктуры актуальными внутренними нарушителями могут являться:

- лица, имеющие права доступа в помещения с техническими средствами информационной инфраструктуры, но не имеющие прав доступа к самим техническим средствам, например, гости или посетители, лица, оказывающие услуги: сантехники, газовики и т. п.;
- легитимные пользователи информационной инфраструктуры, не имеющие прав на обработку защищаемой информации, например, дети;

- лица, обеспечивающие, сопровождение и ремонт технических средств и программного обеспечения, например, компьютерный мастер, к которому Вы обращаетесь.

### 3.3.2. Моделирование угроз информационной безопасности

Исходя из особенностей информационных систем и возможностей актуальных нарушителей, формируется перечень актуальных угроз информационной безопасности. В этот перечень включаются угрозы, которые потенциально могут быть реализованы, и у нарушителей достаточно ресурсов для их реализации.

**Определение 3.3.** *Угроза безопасности информации — это совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке.*

Угрозы безопасности информации можно разделить на объективные, не зависящие от человека, и субъективные (соответственно зависящие от человека) угрозы.

Примерами объективных угроз безопасности информации являются [19]:

1. Утечки информации по техническим каналам. Физические свойства некоторых носителей информации (таких как звуковая волна, световая волна или электромагнитное поле) не всегда позволяют полностью контролировать их распространение. Поэтому при обработке информации возникают угрозы утечки акустической (речевой) или видовой информации, а также утечки информации по каналам побочных электромагнитных излучений и наводок.
2. Дефекты, сбои и отказы, аварии технических средств и программного обеспечения, а также систем «жизнеобеспечения» информационной инфраструктуры.
3. Явления техногенного характера (например, непреднамеренное электромагнитное или радиационное облучение).
4. Природные явления и стихийные бедствия (например, пожары, наводнения, попадания молний, землетрясения).

Примерами субъективных угроз безопасности информации являются [19]:

1. Угрозы съема информации, при ее утечке по техническим каналам (сама по себе утечка предполагает только неконтролируемое распространение информационного сигнала, «съем» предполагает его злонамеренное использование).
2. Угрозы несанкционированного доступа (как к информации, так и к ее носителям).
3. Угрозы разглашения информации (часто их также называют угрозами утечки информации, но в данном случае речь идет скорее о действиях лиц, имеющих доступ к информации, и осознанно передающих эту информации лицам, не имеющим права доступа к ней).

Угрозы несанкционированного доступа могут быть реализованы как внутренними (за пределами контролируемой зоны), так и внешними нарушителями (как за пределами, так и внутри контролируемой зоны), одним из следующих путей (или их комбинацией) [15]:

- путем подключения к техническим средствам и каналам связи;
- путем использования закладочных средств (устройств);
- путем использования штатного программного обеспечения информационной системы (для внутреннего нарушителя);
- путем применения вредоносного программного кода;
- путем хищения носителя защищаемой информации;
- путем реализации компьютерной (для внутреннего нарушителя) или сетевой атаки (например, с помощью анализа сетевого трафика, сканирования вычислительной сети, удаленного запуска приложений, организации отказа в обслуживании, путем посылки большого числа пакетов для обработки).

Угрозы разглашения информации реализуются, как правило, внутренними нарушителями, имеющими права доступа к защищаемой информации, однако могут быть реализованы и внешними нарушителями при условии предварительного получения несанкционированного доступа к защищаемой информации. Угрозы разглашения информации могут быть реализованы следующими путями [15]:

- путем копирования информации на незарегистрированный носитель (например, на неизвестный flash-накопитель);
- путем передачи носителя информации лицам, не имеющим права доступа к ней (например, при ремонте);
- путем утраты (потери) носителя;
- путем передачи информации по открытым каналам связи (в том числе с помощью электронной почты);
- путем обработки информации на незащищенных технических средствах (в том числе на незащищенном домашнем компьютере).

### **3.4. Категорирование, классификация, определение уровней защищенности**

Модель нарушителей и угроз разрабатывается в отношении конкретной информационной системы и должна учитывать её технологические особенности. Например, наличие или отсутствие Wi-Fi модулей, наличие или отсутствие каналов связи, выходящих за пределы контролируемой зоны и другие.

Категорирование или классификация объектов защиты обычно проводится на основании формальных критериев, утвержденных в правовых актах. В таких актах определяются следующие отношения: какая информация является более ценной по отношению к другой или какая информационная система является более



важной по сравнению с другими системами. Категорирование состоит в отнесении объекта информатизации или обрабатываемой на нем информации к определенной категории (классу или уровню защищенности). Например, для персональных данных определяются уровни защищенности, а для государственных информационных систем классы защищенности.

Для определения класса информационной системы или уровня защищенности информации в организациях создается специальная комиссия. Комиссия собирает информацию, необходимую для категорирования объекта информатизации, или заказывает сбор такой информации у сторонних организаций. Далее на основании собранной информации комиссия должна принять решение об отнесении объекта информатизации к той или иной категории. Это решение оформляется специальным актом, например, актом классификации государственной информационной системы или актом определения уровней защищенности персональных данных. Основным параметром для определения категории информации является величина ущерба, который может нанести нарушитель, реализовав угрозу информационной безопасности в отношении этой информации. Категорирование обычно не учитывает технологических особенностей информационных систем.

Рассмотрим в качестве примера порядок определения уровней защищенности персональных данных, обрабатываемых в информационных системах (в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»).

Таблица 3.

Памятка для определения уровней защищенности персональных данных

Тип ИСПДн	Категории субъектов	Число субъектов ПДн	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн, обрабатывающая специальные категории ПДн	Лица, не являющиеся сотрудниками организации	Более 100.000	УЗ 1	УЗ 1	УЗ 2
		Менее 100.000	УЗ 1	УЗ 2	УЗ 3
	Сотрудники организации	Более 100.000	УЗ 1	УЗ 2	УЗ 3
		Менее 100.000	УЗ 1	УЗ 2	УЗ 3
ИСПДн, обрабатывающая биометрические ПДн	Лица, не являющиеся сотрудниками организации	Более 100.000	УЗ 1	УЗ 2	УЗ 3
		Менее 100.000	УЗ 1	УЗ 2	УЗ 3
	Сотрудники организации	Более 100.000	УЗ 1	УЗ 2	УЗ 3
		Менее 100.000	УЗ 1	УЗ 2	УЗ 3
ИСПДн, обрабатывающая иные категории ПДн	Лица, не являющиеся сотрудниками организации	Более 100.000	УЗ 1	УЗ 2	УЗ 3
		Менее 100.000	УЗ 1	УЗ 3	УЗ 4
	Сотрудники организации	Более 100.000	УЗ 1	УЗ 3	УЗ 4
		Менее 100.000	УЗ 1	УЗ 3	УЗ 4
ИСПДн, обрабатывающая общедоступные ПДн	Лица, не являющиеся сотрудниками организации	Более 100.000	УЗ 2	УЗ 2	УЗ 4
		Менее 100.000	УЗ 2	УЗ 3	УЗ 4
	Сотрудники организации	Более 100.000	УЗ 2	УЗ 3	УЗ 4
		Менее 100.000	УЗ 2	УЗ 3	УЗ 4

Уровень защищенности персональных данных определяется на основе четырех критериев:

1. Тип обрабатываемых персональных данных (или тип информационных систем, в которых обрабатываются такие персональные данные). Выделяют четыре типа персональных данных: специальные, биометрические, общедоступные и те, которые не попадают в предыдущие категории — иные.
2. Категория субъектов персональных данных. Выделяют две категории субъектов: субъекты, являющиеся сотрудниками организации — оператора персональных данных, и субъекты, не являющиеся ее сотрудниками.
3. Число субъектов, персональные данные которых обрабатываются. Выделяют две категории: свыше 100.000 субъектов или менее 100.000 субъектов.
4. Тип актуальных угроз безопасности информации. Выделяют три типа актуальных угроз: третий тип соответствует ситуации, при которой угрозы реализуются нарушителями, не проводящими анализ прикладного или системного программного обеспечения на предмет выявления уязвимостей; второй тип угроз предполагает реализацию угроз нарушителями, проводящими анализ прикладного программного обеспечения; первый тип угроз предполагает реализацию угроз нарушителями, проводящими анализ как прикладного, так и системного программного обеспечения.

На основании выбора значений всех четырех параметров определяется уровень защищенности персональных данных. Традиционно наименее критичный уровень (класс, категория) защищенности, требующий реализации меньшего числа мер информационной безопасности, имеет больший индекс (цифру), в данном случае это четвертый уровень защищенности. Наиболее критичным является первый уровень защищенности персональных данных.

Результатом формирования требований к защите информации будут являться модель нарушителя и угроз информационной безопасности, в которой определяются актуальные для информационной системы нарушители и угрозы, которые они способны реализовать, а также акт классификации, в котором указывается категория (класс или уровень защищенности) информационной системы, определённый комиссией. Кроме того, на этом этапе формируется техническое задание на проектирование системы защиты информации, в котором приводится краткое описание информационных систем, перечни актуальных нарушителей и угроз информационной безопасности, а также присвоенные категории (классы или уровни защищенности). Целью создания технического задания на проектирование системы защиты информации является фиксирование основных требований к разрабатываемой на следующем этапе проектной документации.

### **3.5. Проектирование системы защиты информации**

После того, как на этапе моделирования нарушителей и угроз определено, какие нарушители будут нас атаковать и каким образом они будут это делать, необходимо подготовиться к отражению атак. Требуется установить барьеры, которые будут препятствовать нарушителям в осуществлении их планов. В качестве таких барьеров выступают средства защиты информации.

Виды средств защиты информации, конкретные продукты, которые будут использоваться для обеспечения безопасности защищаемой информации, их число,

места расположения, конкретные параметры, а также особенности установки и настройки определяются при проектировании системы защиты информации.

Таким образом, если после моделирования нарушителей и угроз становится понятно, кто и как на нас будет нападать, то после проектирования системы защиты информации должно стать понятно, каким образом мы будем защищаться.

Исторически сложилась ситуация, при которой при создании новых информационных технологий проблемы их безопасности не являются первостепенными. В первую очередь при создании новых технологий внимание уделяется их работоспособности и надежности, удобству использования. Обеспечение безопасности обычно накладывает на информационные технологии дополнительные ограничения, поэтому вопросами безопасности обычно пренебрегают на ранних этапах развития технологии. В последующем недостаток внимания к вопросам обеспечения информационной безопасности приводит к тому, что нарушители находят уязвимости в информационных технологиях и получают возможность реализовать угрозы информационной безопасности. После этого разработчики технологии начинают уделять внимание вопросам обеспечения безопасности, поскольку они в такой ситуации уже обусловлены рынком.

Большое число информационных технологий, а также конкретных продуктов, в которых реализуются эти технологии, порождает большое число уязвимостей и возможностей для нарушителей по их реализации. Соответственно возникает необходимость создания множества средств защиты информации, обеспечивающих безопасность от тех или иных угроз, закрывающих те или иные уязвимости. Поэтому в настоящий момент на рынке представлено очень большое число средств защиты, реализующих разные технологии обеспечения информационной безопасности, необходимые для применения в различных ситуациях. Далее мы рассмотрим основные виды средств защиты информации.

Системы управления доступом обычно состоят из трех элементов: подсистемы идентификации, подсистемы аутентификации и подсистемы авторизации. Подсистема идентификации обеспечивает наличие у каждого легитимного пользователя информационной системы уникального идентификатора и осуществляет контроль наличия предъявляемого идентификатора в базе данных (существующих идентификаторов). Подсистема аутентификации позволяет убедиться, что лицо, обращающееся к информационной системе, может подтвердить, что оно является владельцем предъявляемого им идентификатора (например, с помощью предъявления пароля). Подсистема авторизации позволяет пользователю получить права в информационной системе, которые соответствуют предъявленному идентификатору.

Система управления доступом должна обеспечить возможность доступа к защищаемым ресурсам только для легитимных пользователей информационной системы, обладающих правами доступа к этим ресурсам. Об особенностях управления доступом можно узнать в дополнительных материалах к этой лекции, а также в лекциях, посвященных управлению доступом в операционных системах.

В процессе эксплуатации информационной системы в ней могут происходить различные сбои, а также на неё могут осуществляться атаки. Для того, чтобы корректно обрабатывать эти события, необходима подсистема регистрации и учета (или аудита). Эта система фиксирует события, которые происходят в информационной системе, консолидирует их и предоставляет для анализа системным администраторам или администраторам информационной безопасности. Проводя анализ событий в информационной системе, не всегда можно однозначно определить, что в ней происходит

(или уже произошло). Возможно, в системе происходит какая-то нестандартная процедура (например, обновление программного обеспечения), или в системе произошел сбой, или систему атакуют. Наличие системы регистрации и учета позволяет собирать базу знаний по различным событиям, анализировать накопленные данные и принимать решения о том, что происходит в системе и каким образом следует реагировать на происходящее (в том числе определять какие мероприятия по противодействию атакам следует реализовать в первую очередь). Операционные системы, средства защиты информации и другие программные продукты ведут специализированные журналы, которые (при соответствующей настройке) фиксируют происходящие события, время, в которое они происходят, источники событий, произошедшие при этом ошибки и многое другое.

Системы защиты информации от утечек или DLP-системы очень близки к системам регистрации и учета, но направлены в основном на регистрацию действий пользователей, связанных с передачей информации, копированием ее на отчуждаемые носители, распространением в сети Интернет, отправлением по почте и так далее. DLP-системы фиксируют факты передачи или копирования сообщений. Кроме того, они обладают средствами анализа, позволяющими обнаруживать сообщения, удовлетворяющие определенным условиям. Например, содержат метку «для служебного пользования» или являются копиями документов, содержащих печати и штампы организации или подпись руководителя. Собранную DLP-системой информацию анализирует администратор информационной безопасности или сотрудники службы экономической безопасности. DLP-системы (при соответствующей настройке) также могут сигнализировать об определенных ситуациях или инцидентах, направляя сообщения сотрудникам служб информационной или экономической безопасности. Получив такое сообщение, службы безопасности реагируют в соответствии с установленными в организации регламентами. Примерами систем защиты информации от утечек являются DLP-системы InfoWatch или Zecurion.

Системы обеспечения целостности обычно состоят из двух подсистем. Первая подсистема отвечает за контроль целостности. Например, мы хотим удостовериться, что записанная на жёсткий диск информация осталась неизменной в течение определенного периода времени. Для этого при записи файла на жёсткий диск вычисляется контрольная сумма (или значение хэш-функции) этого файла, которая сохраняется вместе с файлом или на отдельном носителе. Для проверки целостности файла через определенный промежуток времени, требуется снова вычислить контрольную сумму этого файла и сравнить с тем значением, которое было записано в первый раз. Если значения совпадут, то с большой вероятностью файл остался неизменным.

Вторая подсистема необходима для восстановления целостности, в том случае, если первая подсистема сигнализирует о том, что целостность файла нарушена. Подсистема восстановления целостности может быть организована различными способами. С одной стороны, она может использовать методы теории кодирования, которые позволяют восстанавливать определённое число случайных ошибок, которые могли произойти в нашем файле при хранении. Например, магнитные домены на жестком диске могли утратить намагниченность, что не позволит корректно воспроизвести записанную информацию. С помощью теории кодирования можно найти домены, в которых произошли ошибки, и восстановить их исходное значение. С другой стороны, подсистема восстановления целостности может быть организована как совокупность системы резервного копирования и системы восстановления.

Система резервного копирования осуществляет регулярное копирование информации на вспомогательные носители, например, на CD- или DVD-диски, или флеш-накопители. Система восстановления обеспечивает обнаружение последней целостной копии нашего файла (то есть копии, в которой еще не произошли изменения, обнаруженные подсистемой контроля целостности) и восстанавливает наш файл путем «обратной записи резервной копии». Если жёсткий диск еще пригоден для использования, она запишет резервную копию на него, в противном случае предложит записать резервную копию на альтернативный носитель. В качестве примеров подсистем обеспечения целостности приведём систему восстановления операционной системы Windows после сбоев, а также систему резервного копирования Acronis.

Подсистема межсетевого экранирования. Несмотря на то, что сеть Интернет повсеместно используется для обеспечения коммуникаций, мы не можем гарантировать, что посредством этой сети к нам не будет проникать вредоносное программное обеспечение или другой негативный контент. Кроме того, мы не можем гарантировать, что нарушитель, имеющий доступ к сети Интернет, не будет пытаться нас атаковать. Поэтому для того, чтобы обезопасить нашу сеть и отделить её от потенциально опасной среды (например, сети Интернет или других сетей общего пользования) используются межсетевые экраны. Эти средства защиты фильтруют входящий и исходящий трафик по определённым правилам. Например, пропускают информационные пакеты с определёнными заголовками и от определённых источников и не пропускают другие пакеты. Таким образом, с помощью межсетевых экранов можно запретить пропускать в нашу сеть нежелательный трафик (например, содержащий вредоносное программное обеспечение). Кроме того, с помощью межсетевых экранов можно запретить сотрудникам организации обращаться к вредоносным ресурсам, размещённым в сети Интернет. Обнаружив в трафике такие запросы, межсетевой экран не пропустит их в сеть общего пользования и, таким образом, защитит от попадания в нашу сеть нежелательного трафика, который может попасть в неё вместе с ответами на запросы сотрудников.

С развитием технологий межсетевые экраны включают в себя всё новые и новые элементы. Помимо реализации стандартных функций по фильтрации трафика на основе анализа заголовков, IP- и MAC-адресов, межсетевые экраны включают элементы антивирусных средств защиты для контроля отсутствия в проходящем трафике вредоносного программного обеспечения. Кроме того, на настоящий момент межсетевые экраны часто объединяют ещё с одним видом средств защиты информации — системами обнаружения и предотвращения вторжений, позволяющими анализировать трафик на предмет выявления действий активного нарушителя. Примерами межсетевых экранов являются ViPNet Firewall, Рубикон, Checkpoint.

Предположим, что мы отделили с помощью межсетевого экрана нашу вычислительную сеть от вычислительной сети Интернет или аналогичных систем общего пользования. Таким образом, мы установили контроль над своей вычислительной сетью. Однако для нас может быть актуальна задача по обмену информацией с другими организациями или лицами, не подключёнными к нашей вычислительной сети. В этом случае нам придется передавать сообщения через сеть Интернет (или иную стороннюю сеть). Сообщения выйдут за пределы нашей вычислительной сети и мы не сможем их контролировать, в том числе обеспечивать их безопасность теми же средствами и методами, которые применяются внутри вычислительной сети.

Для обеспечения безопасности информации, которая покидает нашу вычислительную сеть, необходимо применять средства криптографической защиты информации. Неформально, с помощью средств криптографической защиты информации можно построить защищенный канал связи сквозь небезопасную вычислительную среду (например, сеть Интернет). Нарушитель сможет обнаружить, что мы обмениваемся информацией с нашим контрагентом, но, получив доступ к передаваемой информации, он обнаружит, что она является криптографически преобразованной. Не зная специальных, хранящихся в секрете, сведений, а именно криптографического ключа, нарушитель не сможет восстановить исходную информацию, то есть сообщение, которое мы зашифровали перед тем, как отправить нашему контрагенту. Кроме построения защищенных каналов связи, необходимых для обеспечения конфиденциальности передаваемой информации, подсистема криптографической защиты информации также позволяет решать задачи обеспечения целостности, аутентификации и другие. К средствам криптографической защиты информации относятся (кроме прочего) средства создания и проверки электронной подписи.

Примерами криптографических средств защиты информации являются продукты технологии VIPNet: программно-аппаратный комплекс VIPNet координатор, программное обеспечение VIPNet Client, а также программно-аппаратные комплексы «Застава» и «Континент», программный продукт «Континент-АП» и другие.

Развитие средств вычислительной техники пошло по пути универсализации. К сожалению, прямым следствием этого подхода является наличие вредоносного программного обеспечения. Теоретически обосновано, что из предположения о том, что наша модель вычислений является достаточно мощной (универсальной), можно заключить, что в рамках данной модели существует программное обеспечение, способное к самовоспроизведению. Это открывает возможности для создания вредоносного программного обеспечения. Примерами вредоносного программного обеспечения являются классические вирусы, троянские программы, сетевые черви, а также шифровальщики. На текущий момент времени вредоносное программное обеспечение в основном попадает в вычислительные сети организаций из сети Интернет. В большинстве случаев оказывается, что сотрудники организации сами допускают ошибочные действия: открывают подозрительные почтовые сообщения или переходят на не проверенные сайты, чем допускают внедрение вредоносного программного обеспечения в вычислительную сеть. По-прежнему актуальным каналом распространения вредоносного программного обеспечения являются зараженные носители информации, например, флеш-накопители. Кроме того, вредоносное программное обеспечение может попасть в вычислительную сеть при подключении сотрудником личного мобильного устройства к рабочему компьютеру.

К сожалению, для файлов большинства известных форматов нельзя утверждать, что они не могут содержать вредоносного программного обеспечения. Вредоносное программное обеспечение может распространяться в текстовых файлах формата docx, файлах изображений, например, JPEG, pdf-файлах и файлах других форматов.

Средства антивирусной защиты используют два основных метода для обнаружения вредоносного программного обеспечения. Первый метод — метод сигнатурного анализа предполагает, что вредоносное программное обеспечение было обнаружено и проанализировано в антивирусной лаборатории. По результатам проведенного анализа устанавливаются идентифицирующие признаки вредоносного программного обеспечения, называемые «сигнатурами». Эти сигнатуры попадают в антивирусные

базы данных. Средство антивирусной защиты анализирует программное обеспечение и данные, попадающие на средство вычислительной техники, на предмет соответствия сигнатурам. Если установлено соответствие сигнатурам программного обеспечения или данных, то они считаются вредоносными, о чём средство антивирусной защиты сообщает пользователю (средства вычислительной техники), при этом оно принимает возможные меры противодействия. Преимуществом сигнатурного анализа является точность идентификации вредоносного программного обеспечения (это безусловно зависит от качества сигнатур). Недостатком сигнатурного анализа является относительно большой интервал времени, который необходим для обнаружения вредоносного программного обеспечения, его анализа в антивирусной лаборатории, создания сигнатуры и обновления антивирусных баз данных. За это время новое вредоносное программное обеспечение может распространиться в сети Интернет и заразить достаточно большое число средств вычислительной техники.

Второй метод — метод эвристического анализа основывается на вероятностных методах. В рамках этого метода по поведению и атрибутам программного обеспечения выдвигается предположение о том, является ли оно вредоносным или нет. При этом возможны ошибки двух родов. Во-первых, при анализе можно сделать предположение о том, что вредоносное программное обеспечение не является вредоносным, следовательно, мы пропустим в нашу вычислительную сеть вредоносное программное обеспечение. Во-вторых, можно предположить, что не являющееся вредоносным программное обеспечение является вредоносным, следовательно, это программное обеспечение можно заблокировать или даже удалить. Вероятностями возникновения ошибок первого и второго родов можно управлять. Рекомендуются настраивать антивирусное программное обеспечение таким образом, чтобы минимизировать ошибки первого рода, то есть уменьшать вероятность принять вредоносное программное обеспечение за безопасное. Примерами антивирусного программного обеспечения являются антивирус Касперского и антивирус Dr. Web.

Далее, для того, чтобы убедиться в защищенности нашей информационной системы или в целом вычислительной инфраструктуры, применяются средства анализа защищенности. Это специальный класс средств защиты, который обеспечивает поиск и анализ уязвимостей в вычислительной инфраструктуре. Примерами такого программного обеспечения являются продукты XSpider и RedCheck. Средства анализа защищенности опрашивают средства вычислительной техники, подключенные к нашей вычислительной сети, и проводят проверку наличия актуальных обновлений, а также осуществляют поиск некорректных конфигураций и настроек. Получая ответы от средств вычислительной техники, они формируют базу данных, в которой сохраняют всю собранную информацию. Анализируя собранную информацию, системный администратор или администратор информационной безопасности получает сведения об обнаруженных уязвимостях (отсутствии обновлений, их закрывающих) или о некорректных настройках и может предпринять меры по их устранению.

Для обеспечения информационной безопасности сложных объектов информатизации (например, вычислительной сети с большим числом компьютеров, с несколькими сегментами, которые могут быть территориально распределены) требуется не уступающая им в сложности (и территориальной распределенности) система защиты информации. Управлять такой системой вручную крайне трудно. Поэтому важным элементом системы обеспечения информационной безопасности сложных систем является подсистема централизованного управления. К сожалению, единого решения для управления системой обеспечения информационной безопасности,

включающей в себя средства защиты от несанкционированного доступа, средства межсетевого экранирования, средства криптографической защиты информации, не существует. Наиболее трудно управлять системой защиты, включающей средства защиты информации различных производителей. Обычно система централизованного управления реализуется производителем для своей продукции, а также, в некоторых случаях, для продукции дружественных ему организаций. Примерами систем централизованного управления средствами защиты информации являются: сервер безопасности для средств защиты от несанкционированного доступа Dallas Lock и ViPNet Администратор, управляющий средствами криптографической защиты информации технологии ViPNet.

На текущем этапе развития информационных технологий сложилась ситуация, при которой является выгодным экономить технические ресурсы, а также обеспечивать надежность и устойчивость информационной инфраструктуры за счет применения сред виртуализации. С помощью таких сред можно создавать виртуальные аналоги серверов, автоматизированных рабочих мест и коммутационного оборудования. При этом в виртуальной инфраструктуре остаются актуальными все угрозы, которые представляют опасность для объектов «реального» мира. Кроме того, для виртуальной инфраструктуры появляются принципиально новые угрозы, связанные с атаками на гипервизор (специализированное программное обеспечение или процесс, отделяющий операционную систему и приложения компьютера от аппаратного обеспечения), на базе которого разворачивается виртуальная среда, а также связанные с вопросами распределения памяти в виртуальной инфраструктуре. Примером системы защиты виртуальной инфраструктуры является продукт vGate. Многие средства защиты, которые использовались для защиты «реальных» объектов, получают в настоящее время виртуальные аналоги. Уже существуют и применяются на практике виртуальные аналоги межсетевых экранов, средств криптографической защиты информации, а также специальные антивирусные решения для защиты виртуальной инфраструктуры и другие.

Большинство из перечисленных ранее средств защиты информации призваны обеспечить безопасность информации от большого числа наиболее вероятных угроз, но, к сожалению, они не смогут противостоять специально подготовленной для Вашей организации атаки. Например, зная особенности настройки установленных у Вас средств защиты, нарушитель может подобрать и использовать при атаке такие действия и операции, которые будут приниматься Вашими средствами защиты как допустимые. Системы обнаружения и предотвращения вторжений призваны обеспечить безопасность информационной инфраструктуры при целенаправленных атаках. Системы обнаружения вторжений могут только детектировать атаки и сообщать о них администратору информационной безопасности. Системы предотвращения вторжений могут посылать управляющие сигналы, изменяющие настройки и порядок обработки информации средствами защиты информации. Например, после получения такого сигнала межсетевой экран может заблокировать все каналы связи в целях отражения атаки. Системы обнаружения и предотвращения вторжений анализируют трафик на предмет обнаружения последовательности действий, характерной для проведения атаки. Например, такой последовательностью действий может быть отправка специально подготовленных сообщений определенного формата. Примером программно-аппаратного комплекса, предназначенного для обнаружения и предотвращения вторжений является ViPNet IDS, примерами программных средств



обнаружения вторжений являются соответствующие модули средств защиты от несанкционированного доступа Dallas Lock или Secret Net Studio.

Средства защиты информации, в том числе системы обнаружения вторжений, генерируют достаточно большой объем информации. Для снижения нагрузки по анализу на администраторов информационной безопасности и системных администраторов необходимо применять средства автоматизированной обработки этой информации. Системы, обеспечивающие сбор информации со средств защиты и ее автоматизированную обработку, в том числе корреляцию событий, получили название SIEM-систем (систем менеджмента информационной безопасности и управления событиями безопасности). Примерами таких систем являются ViPNet TIAS или Maxpatrol SIEM.

### **3.5.1. Типовые проектные решения для систем защиты информации**

При проектировании систем защиты информации из всего многообразия имеющихся средств защиты необходимо выбрать те, которые позволят обеспечить безопасность, защититься от актуальных угроз информационной безопасности, а также окажутся для этого оптимальными по другим характеристикам, например, стоимости.

Рассмотрим автономное автоматизированное рабочее место, не имеющие подключений к каналам связи. Для такого рабочего места обычно являются актуальными внутренние нарушители. Это могут быть либо легитимные пользователи, имеющие доступ к средству вычислительной техники и информационным системам, в состав которых входит рассматриваемое средство вычислительной техники, либо обслуживающий персонал (уборщицы, электрики, сантехники и другие), имеющий право доступа в помещение, в котором расположено автоматизированное рабочее место (соответственно доступ к самому рабочему месту), но не имеющий прав доступа к информационным системам, в состав которых входит рассматриваемое средство вычислительной техники. Обычно для защиты автономных автоматизированных рабочих мест достаточно применения средств защиты от несанкционированного доступа, обеспечивающих управление доступом к этому рабочему месту, и средства антивирусной защиты.

Если автоматизированное рабочее место подключено к сетям связи общего пользования, например, к сети Интернет, то средств защиты от несанкционированного доступа и средств антивирусной защиты будет недостаточно. Как минимум, потребуется обеспечить межсетевое экранирование данного рабочего места от потенциально опасной сети. Обратим внимание, что в данном случае необходимо выбирать программно-аппаратные межсетевые экраны, которые могут быть установлены на границе сети. Достаточно широко распространены так называемые (персональные) сетевые экраны. Это программные решения, устанавливающиеся на средства вычислительной техники. Такие экраны не обеспечивают защиту средства вычислительной техники от атак до момента загрузки операционной системы и старта программного обеспечения сетевого экрана. Пока операционная система компьютера ещё не загружена, нарушитель может попытаться получить доступ к компьютеру из сети Интернет и загрузить на него (по сети) стороннюю операционную систему. После чего, обладая правами в этой (навязанной) операционной системе, нарушитель получит доступ к защищаемым ресурсам, расположенным на компьютере.

При развитии вычислительной сети в ней будет расти число средств защиты информации. Управлять вручную различными средствами защиты информации, установленными на более чем 10-ти рабочих местах, достаточно трудно. Поэтому

возникает необходимость в применении систем централизованного управления средствами защиты информации. Кроме того, еще более трудно вручную контролировать состояние вычислительных сетей с большим числом компьютеров. Например, при обновлении операционных систем часть компьютеров вычислительной сети может обновиться, а часть остаться со старыми операционными системами без обновлений. Таким образом, вторая часть компьютеров окажется уязвимой. Поэтому для больших вычислительных сетей рекомендуется использовать средства анализа защищенности для контроля наличия обновлений и отсутствия уязвимостей, а также отсутствия некорректных настроек программного обеспечения и программно-аппаратных средств вычислительной техники.

При взаимодействии информационных систем посредством общедоступных сетей, например, для передачи информации контрагентам или для обмена информацией между территориально распределенными офисами организации, потребуется обеспечить безопасность информации, передаваемой по открытым каналам связи. Для этого потребуется применение средств криптографической защиты информации.

Для организаций среднего масштаба становятся актуальными направленные атаки. Поэтому актуально применение средств обнаружения и предотвращения вторжений. Кроме того, уже на данном этапе становится актуальным применение SIEM-систем.

При дальнейшем увеличении масштаба организации становится оправданным создание центра обработки данных, в котором будет развернута виртуальная инфраструктура. Следовательно, кроме перечисленных ранее средств защиты информации, возникнет необходимость в применении средств защиты сред виртуализации.

Кроме того, если в информационной системе допускается обработка защищаемой информации с использованием портативных и мобильных технических средств: ноутбуков, планшетов или смартфонов, — то необходимо оснастить их средствами защиты информации. Особое внимание в данном случае следует уделять выбору мобильных технических средств, поскольку для многих устройств, например, устройств с операционной системой iOS, наложенных средств защиты может не существовать.

Результатом разработки системы защиты информации является проектная документация на систему защиты, в которой определяются:

- виды средств защиты информации, которые будут входить в состав системы защиты, например, средства антивирусной защиты, межсетевые экраны, системы обнаружения вторжений;
- конкретные продукты — программно-аппаратные комплексы или программное обеспечение, которые будут применяться, например, в качестве средства антивирусной защиты можно использовать либо антивирус Касперского, либо антивирус Dr. Web, а в качестве средства защиты информации от несанкционированного доступа — либо программное обеспечение Dallas Lock, либо программное обеспечение Secret Net Studio;
- средства вычислительной техники, на которые должно быть установлено программное обеспечение средств защиты информации, места расположения программно-аппаратных комплексов защиты информации;
- параметры установки и настройки средств защиты информации.

Кроме того, в проектной документации могут быть предусмотрены компенсирующие меры защиты информации, в случае, если реализация некоторых основных мер

окажется невозможной (например, в случае, при котором основное программное обеспечение информационной системы окажется несовместимым с программным обеспечением средств защиты информации).

После того как проектная документация разработана, готовится техническое задание на создание системы защиты информации. В нем в соответствии с требованиями проектной документации фиксируются характеристики средств защиты информации, которые необходимо приобрести, их число и параметры установки и настройки.

### **3.6. Разработка организационной и эксплуатационной документации**

Для того, чтобы реализовать систему защиты информации, необходимо подготовить соответствующее документальное обеспечение. Традиционно документальное обеспечение делится на две части. Первая часть касается организационной составляющей системы защиты информации. Организационная документация служит для определения лиц, ответственных за реализацию бизнес-процессов в области обработки и защиты информации, наделения их правами и обязанностями, а также служит для определения подходов к решению задач, связанных с обработкой и защитой информации. Например, в организации могут быть назначены лица, ответственные за организацию и защиту персональных данных и за использование средств криптографической защиты информации, описаны процессы взимания согласия субъекта на обработку его персональных данных и т. п. К организационной документации относятся приказы о назначении ответственных лиц, о создании структурных подразделений, занимающихся вопросами обработки и защиты информации, а также политики, положения и регламенты, определяющие порядок обработки информации и её защиты.

Вторая часть документального обеспечения касается вопросов использования (эксплуатации) средств защиты информации и называется рабочей или эксплуатационной документацией. В этой документации содержатся сведения о порядке установки, настройки, обновления, удаления, обслуживания и ремонта средств защиты информации. В состав эксплуатационной документации входят руководства администратора и пользователя средств защиты информации, а также инструкции по администрированию и эксплуатации средств защиты информации.

### **3.7. Внедрение системы защиты информации**

На основании разработанного проектного решения <sup>2</sup> на систему защиты информации и технического задания на ее создание приобретаются средства защиты информации, после чего осуществляется их внедрение, то есть их установка и настройка на серверах, рабочих местах пользователей и на границах вычислительных сетей (в зависимости от функционального назначения).

Например, на границе вычислительной сети устанавливаются межсетевые экраны, системы обнаружения вторжений, криптографические шлюзы. На серверы и

---

<sup>2</sup>Обратим внимание, что, поскольку технологии развиваются достаточно быстро, проектное решение, разработанное более 3-х лет назад, скорее всего, окажется неактуальным ввиду снятия с производства устаревших средств защиты информации (а также внесения изменений в нормативно-правовую базу). Поэтому создавать систему защиты информации, основываясь на таком решении без его предварительной актуализации, не представляется возможным.

автоматизированные рабочие места устанавливаются средства антивирусной защиты, средства защиты от несанкционированного доступа, средства криптографической защиты информации и другие.

Факт установки средств защиты информации может подтверждаться актом установки. В этом акте указываются:

- технические средства, на которые устанавливаются средства защиты;
- перечень устанавливаемых средств защиты;
- установившее их лицо;
- контактные данные лица, к которому можно обратиться в случае нарушения работоспособности средств защиты и технических средств, на которых они установлены.

Результатом внедрения является готовая к эксплуатации система защиты информации.

### **3.8. Оценка соответствия объекта информатизации**

После того, как система защиты информации внедрена, необходимо проверить ее соответствие техническому заданию и проектной документации, а также убедиться в том, что система защиты обеспечивает нейтрализацию актуальных угроз информационной безопасности.

Для решения этих задач служит этап оценки соответствия. Этот этап может быть Вам знаком под названием «аттестация». Для обеспечения качества создаваемой системы защиты информации, проектирование системы защиты, ее внедрение и оценка соответствия должны проводиться с сотрудниками различных подразделений. Планируется, что в дальнейшем будет установлено нормативное требование, согласно которому оценка соответствия должна будет проводиться сторонней организацией, не принимавшей участия в проектировании и внедрении системы защиты информации.

Аттестация является формой оценки соответствия. Под аттестацией понимается комплекс организационно-технических мероприятий, посредством которого подтверждается соответствие объекта информатизации требованиям по защите информации. Объектами информатизации являются автоматизированные рабочие места, информационные системы, а также помещения.

В рамках процедуры аттестации, на основании разработанных программы и методик, проводятся аттестационные испытания. Рассмотрим методы проверок, которые применяются при проведении аттестационных испытаний:

- экспертно-документальный метод (предполагает проверку наличия и исполнения организационно-распорядительной и эксплуатационной документации, а также к этому методу можно отнести проверку соответствия настройки средств защиты информации проектному решению);
- анализ уязвимостей (предполагает использование специального класса средств защиты информации — средств анализа защищенности в целях выявления уязвимостей в системном и прикладном программном обеспечении);

- осуществление попыток несанкционированного доступа в обход системы защиты информации (имитация действий нарушителя при его попытках атаковать информационную систему).

Важно понимать различия между вторым и третьим методами. Анализ уязвимостей предполагает, что мы ищем известные уязвимости (сертифицированными) средствами анализа защищенности. Эти средства используют различные методы анализа для обнаружения неустановленных обновлений безопасности программного обеспечения, неправильно сконфигурированных программно-аппаратных комплексов и неверно настроенного программного обеспечения, и выдают сведения об обнаруженных уязвимостях. Средства анализа защищенности (в общем случае) не пытаются реализовать атаки и эксплуатировать уязвимости. Также важно, что средства анализа защищенности в отличие от человека не анализируют контекст. Например, папка «Пароли» может оказаться ими не замеченной. Нарушитель при атаке на информационную систему, скорее всего, не будет использовать (сертифицированные) средства анализа защищенности. Он применит так называемый, «хакерский» инструментарий, доступный в сети Интернет, будет использовать эксплойты, то есть программное обеспечение, позволяющее эксплуатировать уязвимости и проникать в информационную инфраструктуру. Таким образом, анализ уязвимостей и испытания системы защиты информации путем осуществления попыток несанкционированного доступа (или тестирование на проникновение) представляют собой связанные, но не взаимозаменяемые методы испытаний.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний. В них фиксируются результаты испытаний (тестирования) установленных средств защиты информации. Испытания включают в себя проверку наличия средств защиты информации, проверку соответствия параметров их установки и настройки проектной документации, проверку корректности работы средств защиты информации и другие виды проверок, описанных в программе и методиках аттестационных испытаний.

После оформления протоколов аттестационных испытаний готовится заключение о соответствии объекта информатизации требованиям по защите информации. В заключении приводятся выводы о положительном или отрицательном результате каждого проведенного испытания, и делается общий вывод (заключение) о соответствии (или несоответствии) объекта информатизации заявленному классу защиты. Если заключение отрицательное (объект информатизации не соответствует заявленному классу), то владельцу или оператору объекта информатизации даются рекомендации по приведению объекта в соответствие. После выполнения рекомендаций аттестация может быть проведена повторно. При положительном заключении (объект информатизации соответствует заявленному классу, все испытания пройдены успешно) выдается аттестат соответствия.

В аттестате указывается, какому классу (или уровню) защищенности соответствует объект информатизации. Ранее в аттестате соответствия также указывался период времени, в течение которого действует аттестат. После истечения этого периода времени необходимо было планировать мероприятия по повторной аттестации, но последние изменения нормативных документов ФСТЭК России принципиально изменили ситуацию. На текущий момент аттестат соответствия выдается на весь период эксплуатации объекта информатизации. Таким образом, информационная система должна проходить процедуру аттестации однократно при её создании.

Очень часто представляется, что аттестат соответствия является альфой и омегой обеспечения информационной безопасности. Такой взгляд не является верным. Во-первых, аттестат соответствия — это документ, который подтверждает, что на момент проведения аттестационных испытаний обеспечивается определенный уровень защищенности объекта информатизации. Любое существенное событие может изменить эту ситуацию. Например, перед процедурой аттестации на объекте информатизации были устранены все известные на тот момент уязвимости. Спустя сутки может появиться новая уязвимость, например, для операционной системы Windows, и объект информатизации, который мы буквально вчера считали защищенным, сегодня становится незащищенным. Во-вторых, поскольку аттестат соответствия на текущий момент выдаётся фактически бессрочно, то ясно, что получение аттестата — это однократная краткосрочная или среднесрочная цель. Долгосрочной целью должно являться поддержание достигнутого уровня защищенности и обеспечение ежечасного соответствия объекта информатизации требованиям по информационной безопасности. Соответственно акцент при обеспечении информационной безопасности должен делаться не на получении аттестата соответствия, а на непрерывном обеспечении заданного уровня информационной безопасности.

Обратим внимание, что в общем случае для информационных систем персональных данных проведение процедуры аттестации не требуется. Однако альтернативных процедур, подтверждающих соответствие информационных систем персональных данных требованиям по защите информации, до настоящего момента не предложено. Поэтому обычно при проведении работ по защите персональных данных завершающим этапом также является аттестация информационной системы (персональных данных).

### 3.9. Эксплуатация

После того, как система защиты информации прошла процедуру оценки соответствия (аттестации), начинается период её эксплуатации, в рамках которого предполагается обновление средств защиты информации, уточнение их настроек, а также вывод из эксплуатации в случае выхода из строя или потери характеристик.

Важной характеристикой средства защиты информации является наличие у него сертификатов соответствия ФСТЭК России и ФСБ России. Эти документы (подтверждающие, что программно-аппаратные комплексы или программное обеспечение действительно являются средствами защиты информации и обеспечивают определенный уровень информационной безопасности) являются срочными и в течение определенного периода времени ранее сертифицированные средства защиты информации могут лишиться этого статуса (потерять сертификат). После того, как средство защиты информации перестало быть сертифицированным, с большой вероятностью его дальнейшая эксплуатация в составе системы защиты информации окажется невозможной.

### 3.10. Лицензирование

Из перечисленных видов деятельности подлежат обязательному лицензированию: проектирование систем защиты информации, внедрение систем защиты информации, аттестация объектов информатизации, а также поддержание системы защиты информации в работоспособном состоянии.

Если в составе системы защиты информации не используются средства криптографической защиты информации, то для осуществления перечисленных видов деятельности необходимо привлекать организацию, обладающую лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации. При использовании в составе системы защиты информации средств криптографической защиты, для осуществления перечисленных видов деятельности (за исключением аттестации) необходимо привлекать организацию, имеющую лицензию ФСБ России на виды деятельности, связанные с применением средств криптографической защиты информации.

### **3.11. Вопросы и задания**

**3.1.** Расположите в правильном порядке этапы работ по обеспечению безопасности информации. 1) Оценка соответствия объекта информатизации. 2) Выявление и анализ информационных активов. 3) Проектирование (разработка) системы защиты информации. 4) Формирование требований к защите информации. 5) Внедрение системы защиты информации. 6) Эксплуатация системы защиты информации.

**3.2.** Пусть не обезличенные персональные данные о состоянии здоровья всех граждан Ярославской области обрабатываются в информационной системе, для которой актуальны угрозы, связанные с эксплуатацией уязвимостей в прикладном, но не в системном программном обеспечении. Какой уровень защищенности должен быть установлен для таких персональных данных?

**3.3.** Пусть не обезличенные персональные данные, в том числе фотографии, сотрудников небольшого (до 10 000 сотрудников) предприятия обрабатываются в системе контроля и управления доступом, для которой актуальны угрозы, не связанные с эксплуатацией уязвимостей в прикладном и системном программном обеспечении. Какой уровень защищенности должен быть установлен для таких персональных данных?

**3.4.** Внешние нарушители реализуют угрозы:

1. Из внешних сетей связи общего пользования.
2. Непосредственно в информационных системах.
3. Из сетей международного информационного обмена.
4. Находясь в пределах контролируемой зоны.

**3.5.** Приведите примеры внешних и внутренних нарушителей.

**3.6.** Какие угрозы являются объективным? Приведите примеры.

**3.7.** Перечислите возможные способы реализации угрозы утечки информации.

**3.8.** Перечислите возможные способы реализации угроз несанкционированного доступа.

**3.9.** Какие средства защиты информации обычно применяются для обеспечения безопасности информации, обрабатываемой на автономных компьютерах?

**3.10.** Какие средства защиты информации позволяют обеспечить безопасность информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны?

**3.11.** Какой вид средств защиты информации позволяет контролировать различные каналы передачи информации: электронную почту, мессенджеры, съемные носители информации?

**3.12.** Дайте определение понятию «аттестация объекта информатизации».

**3.13.** Какой документ дает право обработки информации с указанным в нем уровнем конфиденциальности?

**3.14.** Укажите срок действия аттестата соответствия информационной системы, в которой обрабатывается конфиденциальная информация, в случае, если в ходе ее эксплуатации в нее не вносятся существенные изменения.

**3.15.** Тестирование на проникновение — это скорее:

1. Анализ уязвимостей информационной системы.
2. Испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе.
3. Все перечисленное.



## 4. Архитектура компьютера

**Определение 4.1.** *Цифровой компьютер — это электронное устройство, способное решать определенные задачи, исполняя данную ему последовательность команд (инструкций). Описание последовательности команд, исполнение которых приводит к решению определенной задачи, называется программой.*

Современный цифровой компьютер обычно включает в себя следующие основные элементы:

- центральный процессор (или процессоры);
- основную (оперативную) память;
- вспомогательную память;
- устройства ввода-вывода (клавиатуру, мышь, принтер, веб-камеру и другие).

Эти элементы объединяются с помощью «шины» (единого коммуникационного пространства (набора проводников) для передачи управляющих сигналов, адресов и данных).

В этой теме мы кратко ознакомимся с принципами работы каждого основного элемента.

### 4.1. Процессоры

На рисунке 3 показана структура персонального компьютера с шинной организацией.

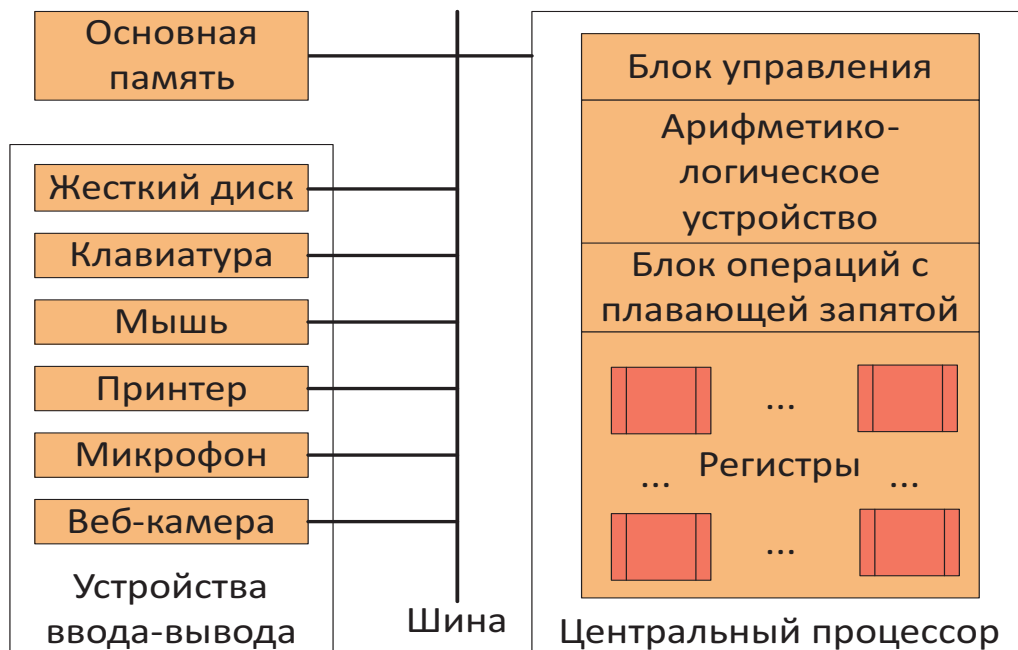


Рис. 3. Схема компьютера

**Определение 4.2.** *Центральный процессор — это основное вычислительное устройство, главная составляющая часть компьютера, его «мозг». Его основной задачей является исполнение машинных инструкций или команд.*

Центральный процессор способен исполнять только небольшой набор простых команд. Такими командами могут являться, например, сложение двух чисел, сравнение двух чисел, чтение данных из памяти или запись в память результата вычислений. Команды, непосредственно исполняемые аппаратным обеспечением компьютера, можно рассматривать как слова, которые в совокупности формируют язык, называемый машинным.

Исполнение команды состоит из трех основных шагов: сначала процессор вызывает команду из памяти, затем определяет ее тип (декодирует), после чего производит соответствующую операцию (действие). За первые два шага отвечает блок управления процессора, а за третью — арифметико-логическое устройство (далее — АЛУ), выполняющее арифметические (например, сложение, вычитание, умножение) и логические (например, «И», «ИЛИ», «Отрицание») операции над «целыми» числами, или блок операций с плавающей запятой (БОПЗ), выполняющий арифметические операции над «вещественными» числами. Описанная последовательность шагов (вызов — декодирование — исполнение) одинакова для всех компьютеров.

Кроме блока управления, АЛУ и БОПЗ, в состав процессора входит самая быстрая в компьютере память, состоящая из нескольких регистров (блоков ячеек памяти) определенного размера (обычно 8, 16, 32 или 64 бита). Регистры необходимы процессору для хранения непосредственно исполняемых им в данный момент команд и обрабатываемых данных. Кроме регистров на микросхеме процессора может размещаться кэш-память, в силу близости к процессору эта память является второй по быстродействию. К сожалению, поскольку микросхема процессора достаточно мала, а на ней необходимо разместить множество элементов, кэш-память является также очень дорогой.

#### 4.1.1. Интерпретация

Чем проще язык, тем проще разработать процессор, способный исполнять команды этого языка, но тем труднее программисту писать на нем программы (поскольку он ограничен возможностями языка). Мы уже знаем, что центральный процессор работает по определенному алгоритму. Следовательно, можно написать программу (имитирующую работу центрального процессора), которая может исполнять другие программы. Такая программа называется интерпретатором. Программы, исполняемые процессором, могут быть исполнены интерпретатором и наоборот, поэтому можно говорить об их эквивалентности.

Таким образом, при разработке компьютеров можно идти по двум принципиально разным путям. Предположим, что мы выбрали машинный язык для нового компьютера. Тогда на следующем этапе необходимо выбрать: будем ли мы разрабатывать физический процессор, непосредственно выполняющий команды нашего машинного языка, или мы разработаем программу-интерпретатор (для программ, написанных на нашем машинном языке) и физический процессор для выполнения этой программы-интерпретатора. По сути, интерпретатор осуществляет «перевод» с выбранного машинного языка на более простой (элементарный) язык процессора. Следовательно, процессор, предназначенный для исполнения интерпретатора, может быть существенно проще, чем процессор, предназначенный для исполнения программ на машинном языке без предварительной интерпретации.

Основное преимущество интерпретации состоит в том, что разработку сложного аппаратного обеспечения можно заменить разработкой сложного программного обеспечения. Копирование же последнего намного проще, чем первого.

В конце 50-х годов 20-го века компания IBM стала первой компанией, которая с помощью интерпретации обеспечила совместимость своих компьютеров из разных линеек (условно большой, средней и низкой производительности). До этого момента аппаратное обеспечение более производительной линейки могло поддерживать команды, которые отсутствовали в машинных языках компьютеров других линеек, и поэтому некоторые программы не могли на них исполняться. Именно для обозначения такой совместимости был введен термин «архитектура». В рамках одной архитектуры может существовать множество различных компьютеров, отличающихся по цене, производительности и другим параметрам, но все они должны обеспечивать исполнение одинаковых программ.

В 70-х годах 20-го века практически все компьютеры использовали интерпретацию. Интерпретаторы позволили разработчикам экспериментировать и создавать все более сложные команды (не внося изменения в аппаратное обеспечение). И, как часто бывает, скоро этот процесс стал самоподдерживающимся, то есть создание набора сложных команд стало представлять самостоятельный интерес, не всегда приносящий пользу разработке компьютера в целом. Кроме того, сама парадигма «единой архитектуры» предполагала разработку единого набора команд для различных по производительности компьютеров, а значит, усложнение набора команд происходило как для высокопроизводительных, так и для малопроизводительных компьютеров. Это привело к тому, что в 80-х годах создались условия, благоприятные для разработки новых процессоров без интерпретации.

#### **4.1.2. Системы RISC и CISC**

В начале — середине 80-х годов 20-го века в университетах Беркли и Стенфорде были разработаны не предполагающие интерпретации процессоры, позже развившиеся в широко известные продукты SPARC и MIPS соответственно. Для обозначения процессоров новой архитектуры в университете Беркли был введен термин «компьютер с сокращенным набором команд» (Reduced Instruction Set Computer, RISC). Этот термин несколько искажает основной смысл (хотя на тот момент времени число команд в RISC-компьютере действительно было не велико), скорее правильно говорить о «компьютере с упрощенным набором команд» или о «компьютере с набором простых и быстрых команд». Антагонистом RISC-компьютера выступал CISC-компьютер — «компьютер с полным набором команд» (Complex Instruction Set Computer), то есть скорее «компьютер с набором сложных команд». Примером CISC-компьютера является, например, Intel Pentium и его аналоги.

При разработке новых процессоров главной задачей было добиться лучшего быстродействия, при этом совместимостью с уже существовавшими на тот момент процессорами было пожертвовано. Первоначально в машинный язык RISC-процессоров включались быстрые команды, то есть команды, которые быстро исполняются. Однако под производительностью компьютера фактически понимается не число исполненных в единицу времени (например, в секунду) команд, а число команд, которые запускаются в единицу времени, поэтому впоследствии в машинный язык RISC-процессоров формировался из быстро запускаемых команд.

Противоречия между RISC и CISC процессорами были преодолены компанией Intel. Начиная с 1989 года (и 486 процессора), команды машинного языка процессоров этой компании разделены на два типа. Самые простые команды (первого типа) исполняются непосредственно процессором, аналогично RISC, а более сложные команды (второго типа) интерпретируются и обрабатываются, так же как в CISC. Поскольку простые

команды встречаются существенно чаще, чем сложные, то производительность при таком подходе не сильно ниже, чем производительность RISC-процессоров, при этом такой подход позволяет обеспечить совместимость с CISC-процессорами, а также позволяет использовать существующее программное обеспечение без внесения в него изменений.

#### **4.1.3. Как можно сделать процессор более производительным?**

Самый простой подход состоит в увеличении тактовой частоты процессора. Неформально процессор можно считать цифровым устройством, состояние которого изменяется в дискретные моменты времени — такты. Чем выше тактовая частота процессора, тем чаще в единицу времени может изменяться состояние процессора и тем быстрее он может выполнять вычисления. К сожалению (или к счастью), разработчики процессоров очень интенсивно использовали описанную возможность повышения производительности, так интенсивно, что на настоящий момент на этом пути практически достигнуты физические пределы развития (например, существенную роль играют квантовая неопределенность и невозможность передачи информации быстрее скорости света). Тем не менее, существуют альтернативные подходы к увеличению производительности процессоров.

Как мы уже знаем, более производительным будет считаться тот процессор, который сможет запустить больше команд в единицу времени. Процессор, способный запустить 1 миллиард команд в секунду, будет иметь производительность  $1 \text{ GIPS} = 10^9 \text{ IPS}$  (Instructions Per Second), независимо от того, сколько времени займет исполнение этих команд. Это означает, что чем больше команд мы можем запустить одновременно, тем выше производительность нашего процессора.

Таким образом, вторым по важности подходом к увеличению производительности процессоров является параллелизм. Существуют два основных варианта параллелизма, нашедших применение в разработке современных процессоров. Первый вариант предполагает реализацию параллелизма внутри одного процессора. Он достигается за счет увеличения числа одновременно обрабатываемых команд и получил название «параллелизм уровня команд». Второй вариант предполагает увеличение числа процессоров (или вычислительных ядер), способных одновременно обрабатывать информацию. Этот вариант получил название «параллелизм уровня процессоров».

Далее мы рассмотрим две параллельные архитектуры процессоров, получивших широкое распространение.

#### **4.1.4. Мультипроцессоры (многоядерные процессоры)**

Мультипроцессоры реализуют концепцию «множественный поток команд, множественный поток данных» (Multiple Instruction stream, Multiple Data stream, MIMD). Неформально в рамках данной концепции несколько независимых процессоров исполняют каждый свой набор команд применительно к своим данным.

В состав мультипроцессора входят несколько процессоров (или вычислительных ядер) и одно пространство памяти, доступ к которому имеют все процессоры.

Поскольку каждый процессор может обращаться к любой области памяти для чтения или записи информации, то могут возникать различные аппаратные ошибки. Например, пусть один процессор записывает в память роман «Мастер и Маргарита», а второй — «Белую гвардию». Если процессоры будут обращаться к одним и тем же областям памяти, то в конечном итоге в области будет записан текст того романа, который будет

записан последним обратившимся к области процессором. В такой ситуации прочесть полностью ни первый, ни второй роман будет невозможно. Избежать возникновения аппаратных ошибок можно на уровне программного обеспечения.

Мультипроцессор относительно просто реализовать. Достаточно соединить единственной шиной несколько процессоров (или вычислительных ядер) и общую память. При такой организации возможно возникновение «состязаний» между процессорами за общий ресурс — шину. Для сокращения числа состязаний каждый процессор снабжается своей локальной памятью. Процессоры в основном работают со своей памятью и в более редких случаях обращаются к общей памяти, что снижает нагрузку на общую шину. Примеры схем мультипроцессоров приведены на рисунке 4.

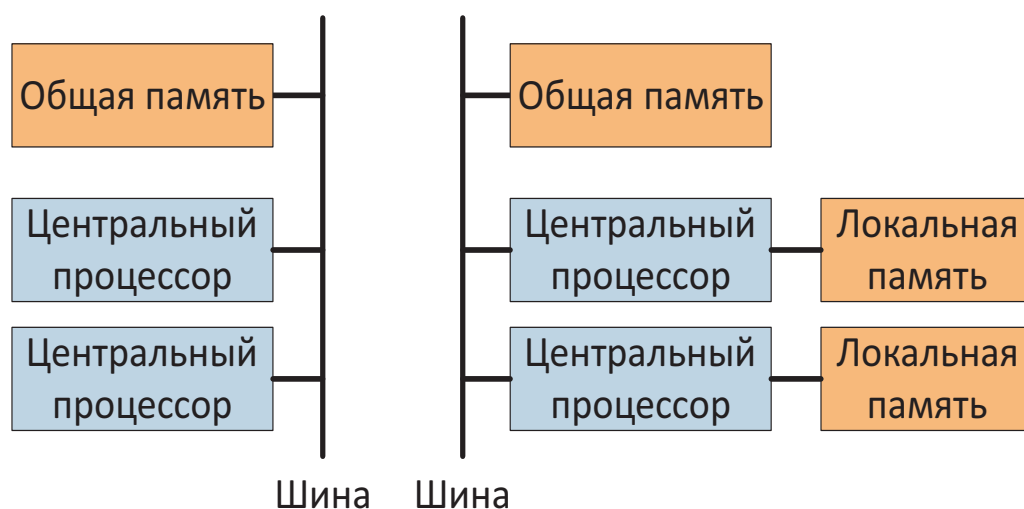


Рис. 4. Мультипроцессор с общей памятью и мультипроцессор с локальной памятью у каждого процессора и общей памятью

Поскольку организовать работу с общей памятью достаточно просто, мультипроцессоры получили очень широкое распространение. С начала 21 века практически все процессоры для потребительского рынка (настольных и портативных ПК, планшетов и смартфонов) являются именно мультипроцессорами.

#### 4.1.5. SIMD-процессоры

Вторая рассматриваемая нами параллельная архитектура реализует концепцию «одиночный поток команд, множественный поток данных» (Single Instruction stream, Multiple Data stream, SIMD). Неформально в рамках данной концепции процессор включает в себя основной управляющий модуль (контроллер) и несколько модулей обработки данных (процессорных элементов). Основной модуль осуществляет вызов и декодирование команд, а также исполняет команды, не связанные с обработкой данных, или инициирует исполнение команд процессорными элементами. Если команда предполагает обработку данных, контроллер передает ее процессорным элементам (всем или группе), после чего каждый элемент исполняет эту команду в отношении своих данных. Каждый процессорный элемент обладает своей памятью.

Ситуации, при которых требуется производить одинаковые действия над различными данными, встречаются достаточно часто. Например, для воспроизведения изображения на мониторе требуется рассчитывать цвет каждого пикселя. При

выполнении компьютерных экспериментов в науке и технике также часто приходится обрабатывать большие массивы информации в соответствии с одинаковыми принципами. Например, необходимо по одному алгоритму обработать данные, полученные при столкновении множества частиц в большом адронном коллайдере. Если данных достаточно много и их можно обрабатывать независимо друг от друга, то применение для обработки SIMD-процессоров может оказаться очень эффективным решением.

Как уже упоминалось, SIMD-процессоры можно эффективно применять для обработки изображений. Это связано с тем, что алгоритмы для обработки изображений обычно хорошо структурированы и предполагают многократное повторение одинаковых действий для различных пикселей, областей экрана, вершин или ребер геометрических фигур. Вследствие этого практически все современные графические процессоры (Graphics Processing Unit, GPU), применяемые в видеокартах, используют SIMD-обработку для обеспечения высокой вычислительной мощности.

На рисунке 5 приведена схема SIMD-процессора.

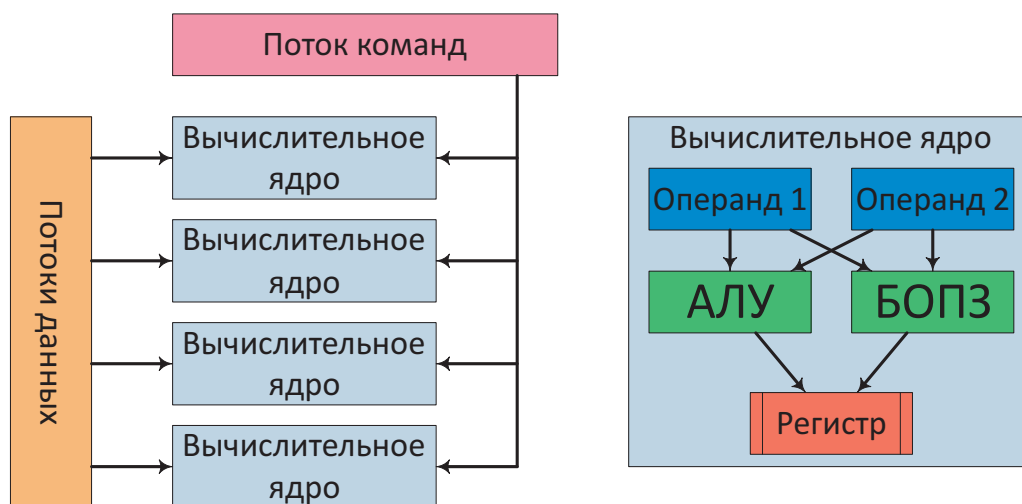


Рис. 5. Схема SIMD-процессора

Команды потокового SIMD-расширения (Streaming SIMD Extension, SSE) для процессоров архитектуры Intel Core позволяют повысить производительность при обработке больших объемов однотипных данных, например, мультимедиа.

## 4.2. Память

**Определение 4.3. Память** — это элемент компьютера, предназначенный для хранения программ и данных.

Память отвечает исключительно за хранение информации (и за целостность при хранении), за изменение (преобразование) информации отвечает процессор.

Базовой единицей измерения количества информации является **бит**. В этом смысле бит равен количеству информации, получаемой при ответе на вопрос, допускающий с равной вероятностью только ответы «да» или «нет».

При хранении информации биту соответствует один разряд двоичной памяти (который также называют битом). Двоичный разряд может принимать только два значения, например, 0 или 1. Это минимальная единица памяти.

Двоичный разряд можно реализовать, основываясь на разности значений какой-либо физической величины. Например, можно принять отсутствие электрического напряжения за 0, а определенное значение напряжения (например, 0,1 Вольта) за 1.

Бит — очень маленькая единица памяти, способная хранить очень небольшое количество информации. Например, с помощью одного бита мы не сможем различить пальцы на одной руке (то есть не сможем присвоить и сохранить имя пальцев). Поэтому для обеспечения эффективной работы биты объединяются в группы, называемые **ячейками**, при этом память представляет собой совокупность ячеек. В настоящий момент широко распространены ячейки, состоящие из 8 бит, называемые **байтами**. Ячейка, состоящая из  $k$  бит, может хранить любое из  $2^k$  двоичных слов длины  $k$ . Соответственно значением байта может являться любое из 256 двоичных слов длины 8.

Каждой ячейке присваивается уникальный номер — адрес, по которому к ней можно получить доступ (обратиться). **Ячейка — минимальная единица памяти, имеющая адрес.** Если память состоит из  $n$  ячеек, то им будут присвоены адреса от 0 до  $n - 1$ . Обычно адреса ячеек представляются двоичными числами. Если мы используем  $m$ -битные адреса, то сможем обратиться к  $2^m$  ячеек памяти. Число бит адреса не зависит от числа бит ячейки. Например, с помощью 32-битных адресов можно получить доступ к  $2^{32}$  ячеек памяти независимо от того, 32 бита в ячейке или 64.

На рисунке 6 показаны различные варианты организации 128-разрядной памяти: 16 ячеек по 8 бит, 8 ячеек по 16 бит или 4 ячейки по 32 бита.

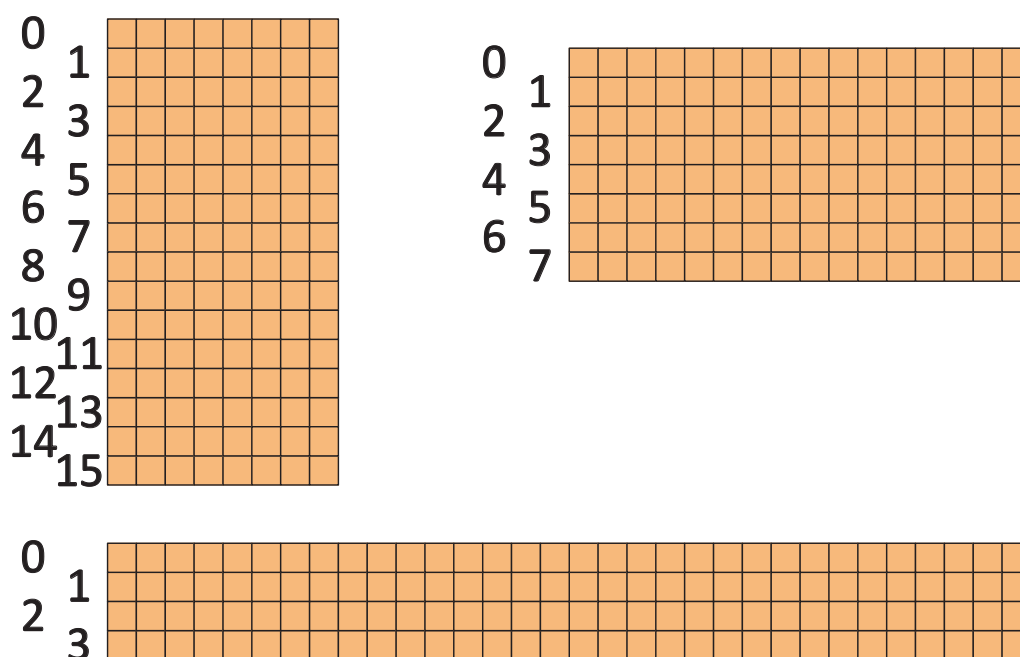


Рис. 6. Варианты организации 128-разрядной памяти

#### 4.2.1. Иерархическая структура памяти

За десятилетия развития компьютерной техники сложилось определенное «противоречие» между подходами к оценке эффективности процессоров и памяти. По традиции процессоры в первую очередь оценивают по производительности, а память по объему (емкости). Соответственно инженеры прилагают существенные усилия

по увеличению этих показателей, поэтому процессоры (в общем случае) работают намного быстрее памяти. Вследствие этого процессор при обращении к памяти получит запрошенное слово только спустя несколько тактов. Чем медленнее память, тем дольше процессор не получит запрашиваемую информацию.

Традиционным подходом к удовлетворению потребности в быстрой и большой по объему памяти является организация памяти в соответствии с иерархической структурой. На вершине такой иерархии находится наиболее быстрая память маленькой емкости. Ниже по иерархии располагается более медленная память большей емкости. Для современного персонального компьютера иерархия памяти выглядит следующим образом:

Таблица 4.  
Иерархия памяти

Уровень иерархии	Тип памяти	Время доступа	Максимальный объем
1	Регистры процессора	Наносекунды	Около ста байт (несколько сотен байт)
2	Кэш-память	Наносекунды	Несколько мегабайт
3	Основная (оперативная) память	Десятки наносекунд	Несколько терабайт (у очень дорогих компьютеров, например, Apple Mac Pro)
4	Твердотельные накопители и магнитные жесткие диски	Десятые доли микросекунд для твердотельных дисков. Микросекунды для магнитных жестких дисков	Несколько десятков терабайт
5	Оптические диски и накопители на магнитной ленте	Доли секунд, секунды (с учетом необходимости помещения носителя информации в компьютер)	Потенциально неограничен

Помимо изменения времени доступа и объема, по иерархии изменяется также стоимость объема памяти. Терабайт основной памяти стоит тысячи долларов, твердотельных накопителей — около ста долларов, жестких магнитных дисков — менее ста долларов.

Далее мы коротко рассмотрим первые четыре уровня иерархии.

#### 4.2.2. Регистры процессора

**Определение 4.4. Регистр процессора** — это блок ячеек памяти, образующий сверхбыструю память.

Регистр состоит из триггеров — электронных устройств, способных длительно находиться в одном из двух устойчивых состояний и изменять их при управляющем воздействии.



Регистры делятся по своему функциональному назначению. Например, существуют следующие регистры. Указатель команд — регистр, указывающий на команду, которую требуется выполнить следующей. Регистры данных, служащие для хранения результатов промежуточных вычислений. Регистры флагов, хранящие текущее состояние процессора.

Обычно все регистры имеют одинаковую длину, превышающую длину ячейки. Например, при 8-битной ячейке памяти разрядность (битность) регистра может составлять 32 или 64 бита. Поэтому в кэш-памяти и основной (оперативной) памяти ячейки группируются в «слова», которые являются минимальной единицей памяти для обработки процессором. Число ячеек в слове определяется отношением разрядности регистров процессора к числу бит в ячейке. Например, пусть ячейка является байтом, тогда для 32-разрядного процессора слово состоит из 4-х байт, а для 64-разрядного процессора из 8-ми байт.

#### 4.2.3. Кэш-память

**Определение 4.5.** *Кэш-память* — быстрая память, промежуточная между регистрами процессора и основной памятью.

Как мы уже упоминали, технологическая возможность создания быстрой, как процессор, памяти существует, но ее необходимо размещать непосредственно на микросхеме процессора. Это означает, что придется увеличить размеры микросхемы, в свою очередь это приведет к ее удорожанию. Кроме того, (по крайней мере, на текущий момент) существуют другие технологические факторы, которые не позволят разместить на микросхеме процессора память большого объема.

Быстрая память небольшого объема, размещаемая на микросхеме процессора или в непосредственной близости от нее (например, в корпусе процессора, но не на его микросхеме), называется кэш-памятью (от английского слова «cash» — «наличные деньги» буквально «деньги под рукой»). Далее мы кратко рассмотрим принцип работы кэш-памяти.

Принцип, лежащий в основе работы кэш-памяти, называется принципом локальности. Его суть заключается в том, что обычно процессор не обращается к ячейкам памяти произвольно, скорее, на протяжении достаточно длительных промежутков времени он работает с небольшими областями памяти (группами близко расположенных ячеек).

Это связано с тем, что в обычной программе большинство команд требуют последовательного исполнения и соответственно располагаются в ячейках памяти (исключением являются команды перехода (буквально «прыжки» — jump) и вызовы процедур, обычно отсылающие к удаленным адресам памяти). Кроме того, значительную часть программы занимают циклы, суть которых состоит в многократном исполнении фиксированного набора последовательно идущих команд.

Основная идея применения кэш-памяти состоит в том, чтобы (руководствуясь принципом локальности) разместить в ней не только данные, которые нужны процессору в данный момент, но и те, которые с большой вероятностью могут потребоваться ему в следующий.

Если процессору требуются данные для обработки, то в первую очередь он обращается к кэш-памяти. Если данные в ней отсутствуют (случается кэш-промах), процессор обращается к основной памяти. В последнем случае процессор получает запрошенные данные, а, кроме того, запрошенные данные вместе с соседними данными

помещаются в кэш-память. Таким образом, повышается вероятность обнаружить необходимые процессору данные в кэш-памяти при его очередном запросе.

Как мы знаем, процессор работает со словами, состоящими из нескольких ячеек памяти. Поэтому, чтобы обеспечить перемещение в кэш-память большего количества данных, чем требуется процессору при одном запросе, кэш-память организуется в виде блоков, состоящих из нескольких слов. Эти блоки называются строками кэша. При кэш-промахе в кэш-память загружается строка из основной памяти, содержащая запрашиваемое процессором слово. Следовательно, основная память также должна поддерживать построчное представление.

Схема подключения процессора с кэш-памятью к основной памяти приведена на рисунке 7.

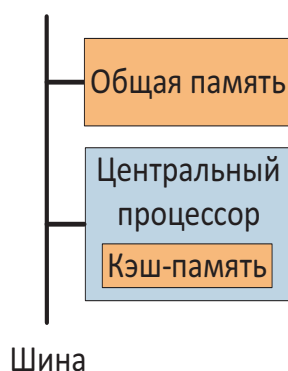


Рис. 7. Схема подключения процессора с кэш-памятью и основной памяти

Чем больше нужных процессору данных «находится» в кэш-памяти, тем меньше среднее время доступа. Например, если процессору за короткий промежуток времени требуется  $k$  раз обратиться к одному слову данных, то при использовании кэш-памяти ему достаточно 1 раз обратиться к медленной основной памяти и  $k - 1$  раз к быстрой кэш-памяти. Для достаточно больших  $k$  выигрыш в производительности стремится к отношению времени отклика основной памяти к времени отклика кэш-памяти.

#### 4.2.4. Основная (оперативная) память

**Определение 4.6.** *Основная (оперативная) память — это энергозависимая память, в которой во время работы компьютера хранятся выполняемые системные (входящие в состав операционной системы) и прикладные программы, а также данные, обрабатываемые этими программами.*

Этот вид памяти имеет принципиально важное значение в силу своего промежуточного положения. С одной стороны, регистры процессора и кэш-память обладают малой емкостью и достаточно дороги, с другой, — время обращения к памяти более низкого уровня иерархии крайне велико. Таким образом, основная память обладает достаточно большой емкостью и относительно приемлемым временем отклика.

В качестве основной памяти для персональных компьютеров наиболее распространена динамическая память с произвольным доступом (Dynamic Random Access Memory, DRAM). DRAM состоит из ячеек памяти, представляющих собой конденсаторы, созданные на основе полупроводниковых технологий. В данном случае различают заряженное и разряженное состояние конденсатора для хранения бита

информации. Со временем заряженный конденсатор разряжается, чтобы не потерять данные, его необходимо динамически «подзаряжать» (отсюда *dynamic*).

Как следует из названия, DRAM позволяет обращаться к произвольным ячейкам памяти. Для этого ячейки группируются в прямоугольные таблицы, состоящие из строк и столбцов. Одна такая таблица называется «страницей», а совокупность страниц — «банком». Обращение к ячейке осуществляется по номеру строки и столбца, на пересечении которых находится ячейка.

Наиболее распространенными типами DRAM на настоящий момент являются DDR3 и DDR4 для обычной оперативной памяти и GDDR6 для оперативной памяти видеокарт.

#### 4.2.5. Жесткие магнитные диски

**Определение 4.7.** *Жесткий магнитный диск (жесткий диск, hard (magnetic) diskdrive, HDD) — это запоминающее энергонезависимое устройство, основанное на принципе магнитной записи.*

Жесткий магнитный диск состоит из одной или нескольких закрепленных друг под другом на вращающейся оси круглых пластин (собственно, дисков), поверхности которых покрыты магнитным слоем. Над каждой поверхностью на кронштейне расположена «считывающая головка». Кронштейны сконструированы таким образом, что позволяют перемещать считывающие головки в направлении к оси, на которой закреплены пластины, или от нее. При работе диска поверхность пластины движется относительно считывающей головки, при этом головка опирается на воздушную подушку и не касается поверхности пластины. При записи информации на головку, содержащую катушку индуктивности, подается переменный ток. Возникающее при этом магнитное поле намагничивает область поверхности, расположенную в этот момент под головкой. При чтении информации головка проходит над намагниченными областями, при этом в ней возникает ток, который можно измерить и тем самым «считать» записанный бит. Рисунок 8 иллюстрирует строение жесткого диска.

При записи на обычные диски магнитные области намагничиваются вдоль окружности диска. В этом случае можно различать, например, намагниченность «по» и «против» часовой стрелки. Более современные технологии перпендикулярной записи позволяют намагничивать магнитные области не горизонтально, вдоль окружности, а вертикально — «в глубь». В этом случае можно различать намагниченность «к» поверхности диска и «от» нее. Экспериментально доказано, что плотность перпендикулярной записи может достигать 370 гигабит на один квадратный сантиметр. Рисунок 9 иллюстрирует особенности продольной и перпендикулярной записи данных на диск.

Поверхность пластин HDD-диска делится на дорожки — концентрические окружности магнитных областей. Дорожки с разных поверхностей, расположенные на одинаковом расстоянии от оси диска, формируют цилиндр. На каждой дорожке выделяются отрезки одинаковой длины — секторы. Сектор является адресуемой областью памяти HDD-диска. Адрес сектора состоит из трех чисел: номера цилиндра, номера головки (или поверхности) и собственно номера сектора.

Конфигурация дорожки диска показана на рисунке 10.

Сектор состоит из преамбулы (*preamble*), необходимой для синхронизации головки перед чтением или записью, области данных и области кода, исправляющего ошибки. Между соседними секторами находится пространство, которое не используется для записи данных, — межсекторный интервал. На соседних дорожках обычно содержится

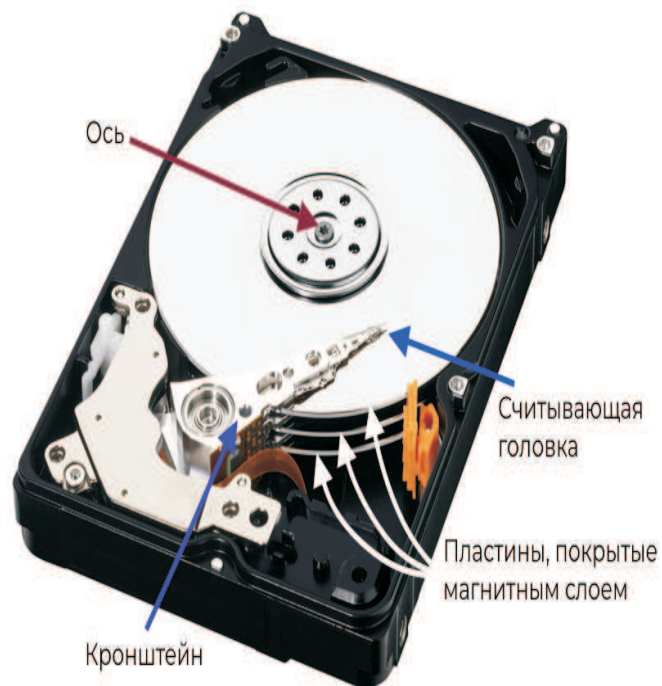


Рис. 8. Строение жесткого диска

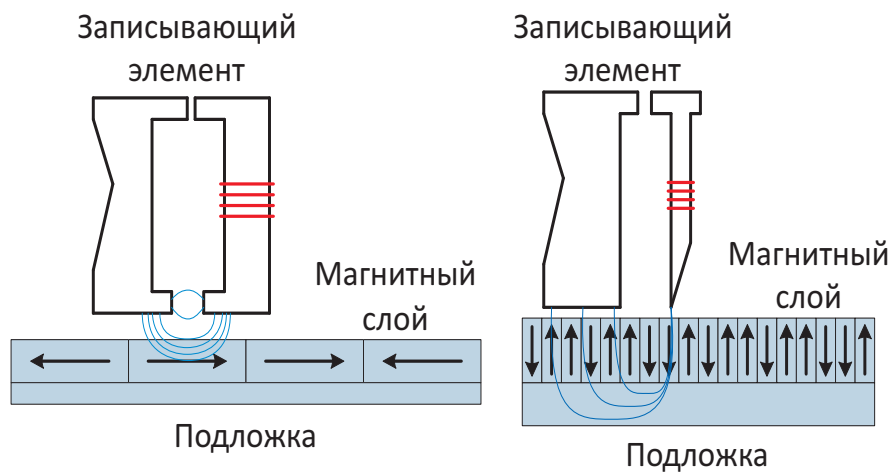


Рис. 9. Продольная и перпендикулярная запись

одинаковое число секторов, но поскольку одна из них обязательно длиннее, то часть дорожки не будет использоваться для записи информации. Эта часть дорожки и будет использована для формирования межсекторных интервалов.

HDD-диском управляет особый процессор — контроллер. Контроллер получает от операционной системы команды на операции с HDD-диском (например, read или write), управляет вращением пластин и перемещением кронштейнов, обнаруживает и исправляет ошибки, а также управляет передачей данных.

С появлением в середине 80-х годов «устройств со встроенным контроллером» (Integrated Drive Electronics, IDE) контроллер диска стал располагаться на самом HDD-

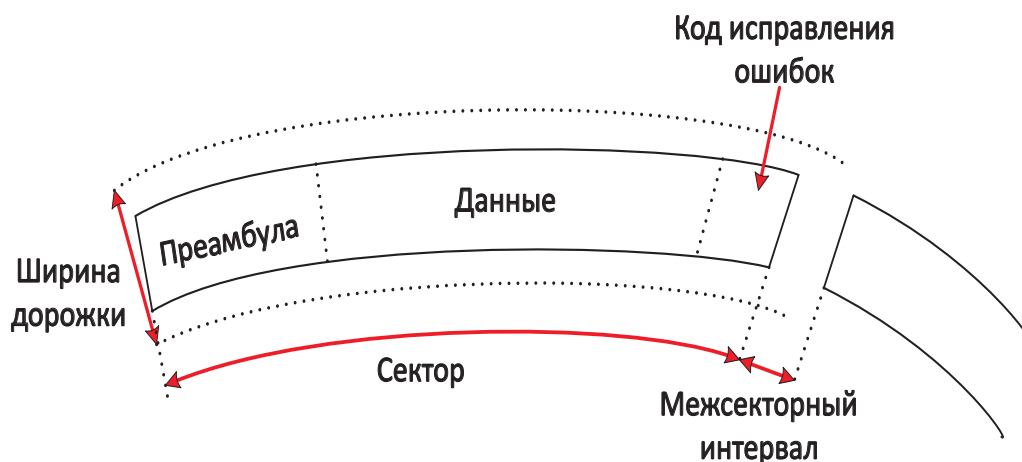


Рис. 10. Фрагмент дорожки диска

диске, а не на плате расширения. При этом на материнской плате стал располагаться IDE-контроллер, роль которого состояла не в непосредственном управлении HDD-диском, а в обеспечении обмена информацией с ним (в том числе передаче контроллеру диска управляющих команд от операционной системы). При этом именно IDE-контроллер обеспечивал подключение HDD-диска к шине, в том числе «захватывал» ее для передачи информации.

IDE (альтернативное название ATA, Advanced Technology Attachment) является интерфейсом (каналом) параллельного подключения HDD-дисков и оптических приводов (для CD- или DVD- дисков) к компьютеру. Стандарт IDE несколько раз совершенствовался, после чего был заменен «наследником» — последовательным интерфейсом обмена данными SATA (Serial Advanced Technology Attachment), который используется в большинстве современных компьютеров. Стандарт SATA можно считать 7-й редакцией стандарта IDE/ATA. В третьей версии SATA (2008 год) позволяет передавать до 6 гигабит в секунду. Для сравнения в 6-й версии стандарта IDE/ATA (2001 год) скорость передачи данных составляла 0,8 гигабит в секунду.

#### 4.2.6. Твердотельные накопители

В начале 1980-х годов Фудзио Масуока, используя эффект, который до этого рассматривался только как механизм «поломки» транзисторов (полупроводниковый прибор), изобрел новый вид памяти — флэш-память. Использованный эффект называется «инжекция горячих носителей». Неформально он состоит в том, что транзистор, использование которого основано на способности переключаться между двумя состояниями, при попадании электрического заряда может навсегда перейти в одно более неизменяемое состояние (и тем самым выйти из строя). Фудзио Масуока показал, что описанный эффект можно использовать для записи информации. Мы не будем останавливаться на устройстве флэш-памяти, поскольку это потребовало бы описания многих технических деталей, скажем только, что флэш-память состоит из транзисторов с плавающим затвором.

**Определение 4.8.** *Твердотельный накопитель (Solid-State Drive, SSD, SSD-диск) — это запоминающее энергонезависимое устройство на основе микросхем памяти.*

SSD-диски являются электронными устройствами и поэтому обладают большей (на настоящий момент в несколько раз) производительностью по сравнению с HDD-дисками, в которых используются механические элементы.

Кроме того, отсутствие движущихся механических элементов, которые легко повредить при переносе, делают SSD-диски наиболее подходящими для портативных и мобильных устройств.

Основным недостатком SSD-дисков на текущий момент является их большая стоимость по сравнению с HDD-дисками. Несмотря на уменьшение стоимости с течением времени, разрыв все еще составляет десятки раз. Как и в общем случае, производители компьютеров пользуются принципом иерархической организации памяти. На текущий момент во многих компьютерах SSD- и HDD-диски используются совместно, при этом SSD-диски занимают 4-й уровень иерархии, а HDD-диски 5-й (съемные носители, при таком рассмотрении, переходят на 6-й уровень). В перспективе SSD-диски могут полностью заменить HDD-диски, но возможно иерархический подход окажется эффективным и будет использоваться на протяжении длительного времени.

Еще одним недостатком SSD-дисков можно назвать постепенное изнашивание основных электронных элементов (транзисторов) при каждом цикле перезаписи информации. При каждом изменении состояния транзистора он приближается к выходу из строя. Для обеспечения надежности и более длительного срока работы запись данных на SSD-диск осуществляется равномерно. Для этого каждый раз для записи выбирается область памяти, которая давно не использовалась. Благодаря такому подходу для обычных пользователей описанный недостаток SSD-дисков не имеет практического значения.

## 4.3. Устройства ввода-вывода

### 4.3.1. Шины

В корпусе современного компьютера (ПК, ноутбука, планшета или смартфона) находится основная «материнская» плата, внутри которой проходят проводники (токопроводящие каналы), образующие специальную коммуникационную среду — шину (или несколько шин). К шине (непосредственно или через специальные разъемы) подключаются процессор (процессоры), оперативная память, вспомогательные микросхемы, а также различные устройства ввода-вывода. Шина используется для передачи данных между элементами компьютера.

**Определение 4.9.** *Компьютерная шина — это единое коммуникационное пространство (набор проводников), служащее для передачи данных между элементами компьютера.*

На рисунке 11 приведена логическая структура персонального компьютера с одной шиной. В таком компьютере центральный процессор, память и устройства ввода-вывода одновременно (параллельно) подключены к шине.

Любое устройство ввода-вывода имеет управляющий элемент — контроллер. Контроллеры устройств ввода-вывода могут располагаться на материнской плате, плате расширения, подключаемой в разъем шины, или входить в состав самого устройства. В случае расположения контроллера на материнской плате он связывается с устройством через соответствующий разъем (материнской платы).

Контроллер не только управляет своим устройством ввода-вывода, но и обеспечивает доступ к шине для передачи данных.

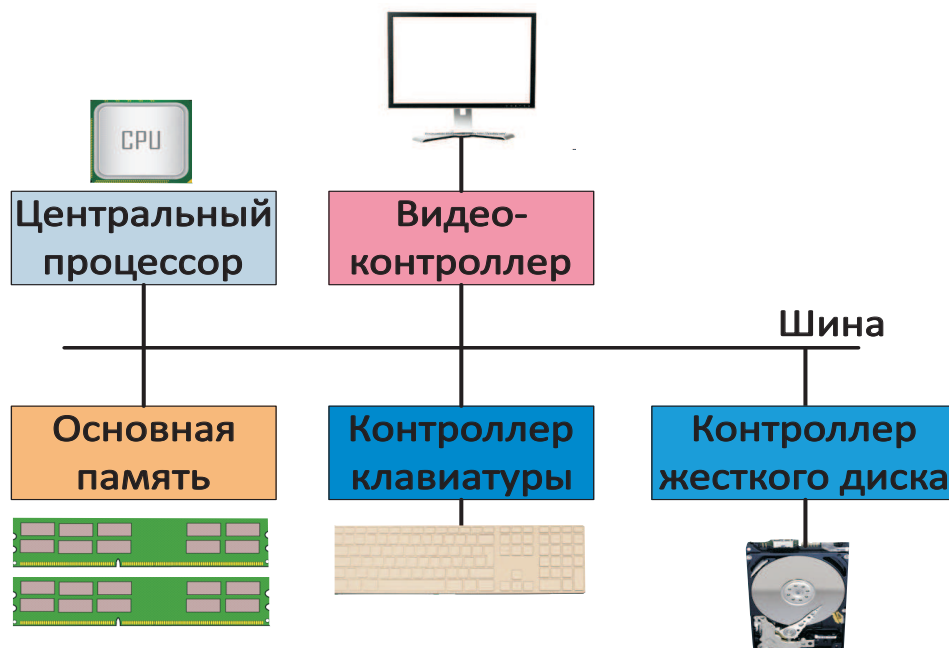


Рис. 11. Логическая структура обычного персонального компьютера

На доступ к шине могут одновременно претендовать процессор и несколько контроллеров устройств ввода-вывода. В таком случае специальная микросхема — «арбитр шины» определяет, кто получит доступ в данный момент. Подключаемые к шине устройства обычно имеют разные приоритеты в захвате шины. Так, устройства ввода-вывода могут «потерять» информацию, если вовремя не получают доступ к шине (например, пользователь нажмет и отпустит клавишу на клавиатуре, сетевая карта полностью использует встроенный объем памяти для хранения полученных из сети Интернет данных и т. п.). Во избежание описанных потерь устройства ввода-вывода обычно имеют более высокий приоритет в захвате шины.

Архитектура компьютера с одной шиной «ISA» (Industry Standard Architecture, промышленный стандарт шинной архитектуры) использовалась в персональных компьютерах с начала 80-х до середины 90-х годов 20 века. В момент ее появления элементы компьютера были еще достаточно медленными и не сильно отличались друг от друга по быстродействию. Поэтому архитектура была достаточно эффективна. Однако экспоненциальный рост производительности центральных процессоров, а также ускорение работы памяти и отдельных устройств ввода-вывода привели к тому, что шина ISA стала узким местом. Естественным желанием было бы заменить шину ISA на более эффективную, но часть устройств ввода-вывода оставалась очень медленной, например, клавиатуры и принтеры, а пользователи не планировали отказываться от этих устройств.

В итоге компьютеры стали производить с несколькими шинами: старой шиной ISA для поддержки медленных устройств и новой шиной PCI (Peripheral Component Interconnect — подключение периферийных компонентов), разработанной компанией Intel.

В наиболее распространенных реализациях шины PCI процессор не взаимодействует с основной памятью посредством этой шины. Вместо этого процессор подключается по выделенной высокоскоростной «шине памяти» непосредственно к контроллеру

памяти. Таким образом, в данной конфигурации к шине PCI подключаются только периферийные устройства.

В начале 20-го века шина PCI была заменена шиной PCI Express (сокращенно PCIe). И, как ранее с шиной ISA, многие современные компьютеры поддерживают и шину PCI (для подключения старых и медленных устройств), и шину PCIe (для новых и быстрых устройств).

Архитектура шины PCIe представлена на рисунке 12.

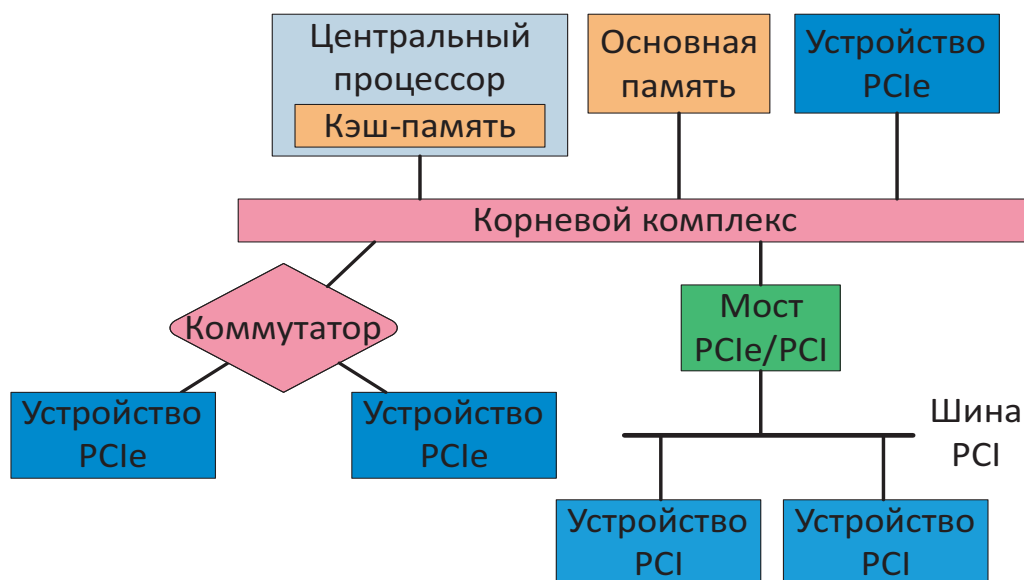


Рис. 12. Архитектура шины PCIe [20]

Несмотря на похожее название, шина PCIe принципиально отличается от шины PCI в части организации связи между устройствами.

Во-первых, по организации работы она ближе к вычислительным сетям, чем к шинам предыдущих поколений. Если процессор хочет обратиться к устройству, он не захватывает шину, а направляет этому устройству пакет данных. Пакет проходит через специальный коммутатор и достигает устройства, после чего осуществляется передача данных. Все устройства напрямую соединяются с коммутатором, образуя звезду.

Во-вторых, для подключения устройств по стандарту PCIe используются двунаправленные последовательные соединения типа «точка-точка», имеющие разрядность 1 бит, и называемые «линиями». Для сравнения, в стандарте PCI все устройства параллельно подключались к 32-разрядной двунаправленной шине.

За единицу времени (такт шины) по линии шины PCIe можно передать всего один бит информации, в то время как по 32-разрядной шине PCI сразу 32 бита. Фокус в том, что за счет простоты физического устройства линии шины PCIe удастся существенно повысить тактовую частоту, то есть такт шины PCIe существенно меньше такта шины PCI.

Рассчитаем максимальную скорость передачи информации по шине PCI. За один такт по шине PCI можно передать 32 бита информации, а ее тактовая частота не превышает 66 МГц. Поэтому скорость передачи данных составляет:

$$[\text{Количество информации, передаваемой за один такт}] \cdot [\text{Число тактов в одной секунде}] = 32[\text{бита}] \cdot 66[\text{МГц}] = 2112[\text{Мбит/с}] = 264[\text{Мбайт/с}].$$



Тактовая частота первой версии шины PCIe составляла около 2,5 ГГц, что обеспечивало скорость передачи информации по одной(!) линии

$$1[\text{бит}] \cdot 2,5[\text{ГГц}] = 2500[\text{Мбит/с}] = 312,5[\text{Мбайт/с}].$$

При этом устройства могут подключаться не по одной, а по нескольким независимым линиям шины, что кратно увеличивает пропускную способность. В 2021 году ожидается обновление стандарта PCIe, в соответствии с которым тактовая частота может достигнуть 64 ГГц, а скорость передачи данных по одной линии шины — 7,877 Гбайт/с. Такая скорость может требоваться программным комплексам, рассчитывающим сложные математические модели, или приложениям дополненной или виртуальной реальности.

### 4.3.2. Клавиатуры

**Определение 4.10.** *Клавиатура* — это устройство ввода информации, состоящее из упорядоченного набора кнопок (клавиш).

Существует достаточно большое число видов клавиатур: мембранная, резиновая, резиномембранная, ёмкостная, механическая, магнитная и проекционная. В настоящий момент в отношении персональных компьютеров наибольшее распространение получили резиномембранные клавиатуры. Далее мы кратко рассмотрим их устройство.

Можно сказать, что резиномембранная клавиатура имеет три основных слоя. Первый слой формируют клавиши, представляющие собой «крышечки», крепящиеся на вертикальные пластиковые стержни, с колпачком внизу. Второй слой формирует эластичный материал (резина или силикон), основная задача которого — предотвращать случайные соприкосновения элементов первого и третьего слоев. Третий слой представляет собой печатную плату, на которую нанесены токопроводящие дорожки. При нажатии клавиши стержень сначала соприкасается с материалом второго слоя, а затем продавливает его через специально предусмотренные для этого отверстия и замыкает контакты на печатной плате. При замыкании и размыкании контактов на клавиатуре вызывается «процедура прерывания»: операционная система компьютера получает сигнал о том, что она должна обработать внешнее событие и запускает специальную программу — обработчик прерывания, которая «идентифицирует» событие, в частности, определяет номер нажатой или отпущенной клавиши.

Например, пока мы удерживаем клавишу Shift, мы будем набирать заглавные символы, при отпущенной клавише Shift символы будут набираться строчными.

На рисунке 13 приведены элементы резиномембранной клавиатуры.

### 4.3.3. Мыши

**Определение 4.11.** *Мышь* — это координатное устройство ввода информации, служащее для управления курсором и выбора команд из «выпадающих меню».

Основная задача, которую решает мышь, состоит в обеспечении возможности указания определенной позиции на экране компьютера. При движении мыши (например, при движении по столу или коврику) курсор на экране также перемещается, что позволяет наводить его на определенный элемент экрана. В состав мыши входят несколько кнопок, нажатие которых позволяет вызывать «меню», связанные с теми или иными элементами экрана, и делать выбор команд из имеющегося перечня (меню).



Рис. 13. Элементы резиноmemбранной клавиатуры

Исторически существовало несколько видов мышей: механические, оптические и оптомеханические, однако оптические мыши фактически вытеснили все остальные виды. Поэтому мы кратко рассмотрим только устройство победившего вида.

В нижней части современной оптической мыши располагаются светодиод (или полупроводниковый лазер) и очень маленькая и быстрая видеокамера. Эта видеокамера снимает несколько тысяч кадров в секунду с разрешением от  $16 \times 16$  до  $40 \times 40$  пикселей. Сравнение нескольких снятых соседних кадров позволяет определить направление перемещения мыши и величину смещения. Освещение поверхности светодиодом позволяет облегчить решение последней задачи.

Обычно при прохождении мышью определенного расстояния (например,  $0,3 \text{ мм}$ ) компьютеру передается последовательность из нескольких байт, в которой передается информация о смещении мыши по оси  $Ox$  и по оси  $Oy$ , а также информация о состоянии кнопок мыши (например, нажаты они или нет).

Информация о перемещениях мыши и состоянии ее кнопок обрабатывается низкоуровневым программным обеспечением (входящим в состав операционной системы), при этом информация об относительных движениях служит для определения позиции на экране, в которой должен появиться курсор. Если кнопка мыши нажата, то, зная положение курсора на экране, компьютер может вычислить, какой элемент должен быть выбран.

#### 4.3.4. Плоские мониторы

**Определение 4.12.** *Монитор* — это устройство вывода информации, отображающее (визуализирующее) данные, полученные от других устройств компьютера.

Необходимость создания плоских мониторов была обусловлена потребностью компактных решений для портативных устройств (не только ноутбуков или портативных компьютеров, но и, например, калькуляторов). Первые плоские мониторы были созданы на основе технологии жидких кристаллов в 60-х годах 20-го века. Их характеристики — компактность и небольшое потребление энергии — позволили практически полностью отказаться от полногабаритных мониторов на основе электронно-лучевых трубок.

На текущий момент жидкокристаллические мониторы остаются самыми распространенными в сегменте пользовательских компьютеров (не только для стационарных компьютеров и ноутбуков, но и для мобильных устройств, планшетов

и смартфонов). Существует большое число различных модификаций технологии жидких кристаллов. Для простоты изложения мы кратко опишем принцип работы монохромного (черно-белого) жидкокристаллического монитора. Работа цветных мониторов основана на тех же принципах, но требует отдельной обработки красного, зеленого и синего цветов.

Жидкие кристаллы — это молекулы, имеющие структуру кристалла, но при этом обладающие свойством текучести, как жидкости. Впервые они были открыты в Австрии ботаником и химиком Фридрихом Рейницером в 1888-м году.

При определенных условиях оптические свойства жидких кристаллов будут зависеть от направления освещения и поляризации света. Воздействуя электрическим полем на линии жидких кристаллов, можно управлять интенсивностью пропускаемого ими света, то есть делать некоторые области монитора более светлыми или темными.

Жидкокристаллический монитор состоит из ЖК-матрицы, источников света (для освещения матрицы изнутри), проводов (проводников, электродов) и корпуса. ЖК-матрица состоит из двух параллельных пластин из стекла или гибких полимерных материалов. В герметичном пространстве между пластинами ЖК-матрицы находятся жидкие кристаллы. На каждую пластину ЖК-матрицы нанесен поляроид (поляризационный фильтр), поскольку жидкие кристаллы чувствительны к поляризации света. Для управления состоянием жидких кристаллов к каждой пластине подключаются электроды. Изображение на мониторе формируется за счет воздействия различным напряжением в разных областях ЖК-матрицы.

Общая структура жидкокристаллического монитора приведена на рисунке 14.

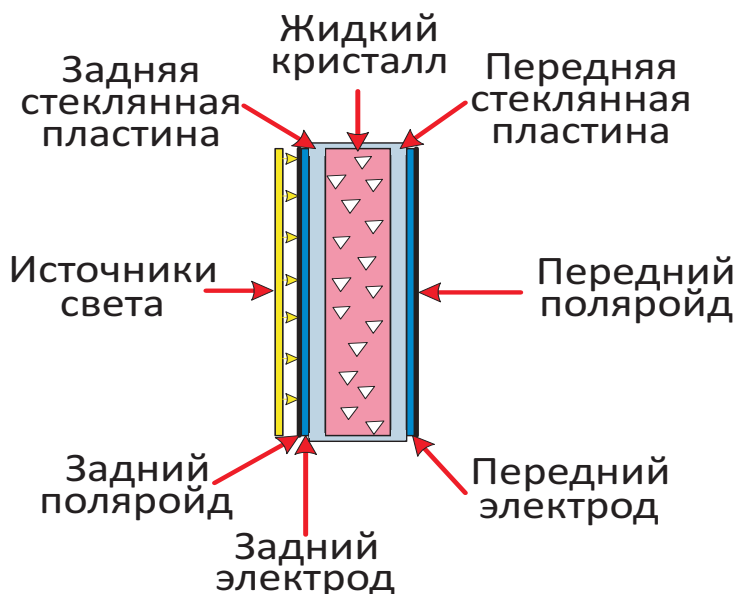


Рис. 14. Структура жидкокристаллического монитора

#### 4.3.5. Сенсорные экраны

**Определение 4.13.** *Сенсорный экран* — это устройство ввода информации, представляющее собой реагирующий на прикосновение экран.

Первый сенсорный экран был разработан сотрудником компании Royal Radar Establishment Эриком Джонсоном в Великобритании в 1965-м году. В начале 70-х годов

20-го века преподаватель Самюэль Херст из Университета штата Кентукки впервые представил графический планшет с возможностью сенсорного ввода, а в 1975-м году он получил патент на резистивный сенсорный экран.

Рассмотрим принципы работы двух основных видов сенсорных экранов, получивших распространение в мобильных устройствах — резистивных и емкостных.

Резистивный сенсорный экран состоит из двух основных слоев, разделенных слоем диэлектрика (изолятора). Верхний слой является гибким, поскольку на него должен нажимать пользователь, а нижний слой жестко закреплен на экране. Оба слоя содержат большое число проводников («проводков»). Для простоты можно считать, что на верхнем слое проводники расположены горизонтально, а на нижнем вертикально.

При нажатии на экран проводники верхнего слоя соприкасаются (или сближаются) с проводниками нижнего слоя, что влияет на электрические параметры системы и позволяет определить область нажатия.

Резистивные экраны обладают хорошей чувствительностью, а кроме того, просты в изготовлении и достаточно дешевы, поэтому получили широкое распространение.

К минусам резистивных экранов можно отнести плохое светопропускание (что требует больших затрат на подсветку), невозможность определять силу нажатия, а также проблему «двоения». Последнюю проблему можно проиллюстрировать следующим примером. Представим, что на экране изображен квадрат, координаты вершин которого равны (0, 0), (0, 5), (5, 0) и (5, 5). При одновременном нажатии на вершины с координатами (0, 0) и (5, 5) будут изменяться параметры тех же проводников, что и при нажатии на вершины с координатами (0, 5) и (5, 0). Таким образом, эти ситуации оказываются неразличимыми.

Распознавать несколько точек нажатия способны так называемые мультитач-экраны (multi-touch). Наибольшее распространение в планшетных компьютерах и смартфонах получили мультитач-экраны, созданные по проекционно-емкостной технологии.

Как и резистивные, проекционно-емкостные сенсорные экраны состоят из двух разделенных диэлектриком слоев, нанесенных на стеклянную основу. Один из основных слоев содержит горизонтально расположенные проводники, а второй — проводники, которые расположены вертикально. Проводники в сенсорном экране должны хорошо пропускать свет (быть прозрачными), поэтому они делаются из особого прозрачного сплава оксида индия и оксида олова.

Приблизительно можно считать, что проекционно-емкостной экран представляет собой множество конденсаторов (устройств, способных накапливать электрический заряд, в простом случае представляемых в виде двух пластин электродов, разделенных слоем диэлектрика), образовавшихся в местах пересечения горизонтальных и вертикальных проводников.

Тело человека хорошо накапливает электрический заряд (вспомните свой жизненный опыт со статическим электричеством). Поэтому прикосновение пальцем (пальцами) к экрану изменяет емкость всех «конденсаторов» в области нажатия. Это изменение можно измерить, что позволяет определить координаты области нажатия.

Проверьте, какой тип экрана у вашего смартфона? Будет ли он реагировать при прикосновении пальцем в резиновой перчатке или при прикосновении карандашом?

Преимуществами проекционно-емкостных экранов являются высокая скорость отклика при касании, поддержка мультитач и возможность определения силы нажатия. Этот вид экранов имеет большую надежность, что обеспечивает более продолжительный срок службы. К недостаткам экрана можно отнести возможность

управления только пальцами, что, например, ограничивает возможности рисования, или специальными стилусами.

#### 4.3.6. Принтеры

В этом параграфе мы кратко рассмотрим только наиболее часто используемые черно-белые лазерные принтеры.

**Определение 4.14.** *Принтер* — это устройство вывода текстовой или графической информации на твёрдый физический носитель (обычно бумагу, но, возможно, ткань, полимер и т. п.).

Схема работы лазерного принтера показана на рисунке 15.

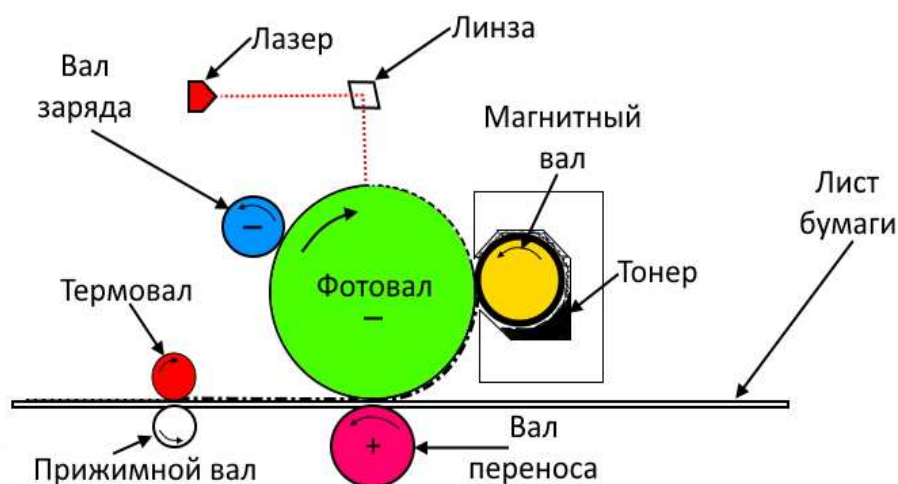


Рис. 15. Схема работы лазерного принтера

Основной частью принтера является вращающийся фотовал. Перед печатью новой страницы фотовал «электризуется» (на него буквально наносят заряженные частицы). Затем поверхность фотовала освещается лазером, таким образом, что формируется линия, состоящая из освещенных и не освещенных лучом лазера точек. Точки, освещенные лазером, разряжаются. После того как линия создана, фотовал поворачивается для формирования следующей линии. Далее линия достигает магнитного вала, к поверхности которого притягиваются частицы тонера. Тонер притягивается к заряженным точкам на фотовале. Таким образом, на фотовале проявляется невидимое ранее изображение.

Теперь линия с тонером приближается к бумаге. Вал переноса заряжает листы бумаги, и тонер притягивается к ним, так же как ранее притягивался к фотовалу. Затем лист с тонером проходит через термовал, расплавляющий тонер и закрепляющий таким образом изображение на бумаге. После этого фотовал разряжается и очищается от остатков тонера. Цикл повторяется.

Кроме уже упомянутых элементов в состав лазерного принтера входит контроллер и до нескольких гигабайт памяти для хранения печатаемых изображений и различных шрифтов, которые могут быть встроенными или загружаться из памяти компьютера.

Принтеры могут получать печатаемые изображения в битовом представлении, но большинство управляются командами специализированных языков описания страниц. Примером такого языка является PostScript, разработанный компанией Adobe.

#### 4.3.7. Веб-камеры

**Определение 4.15.** *Веб-камера* — это цифровая видео- или фотокамера, способная в реальном времени фиксировать изображения реальных объектов на матрице светочувствительных элементов.

Как устроена и как работает веб-камера?

В состав веб-камеры входят следующие элементы: объектив, оптический фильтр, ПЗС-матрица, плата видеозахвата (блок оцифровки), процессор, включающий модуль сжатия видеоизображения, оперативная память и флэш-память, сетевой или USB интерфейс и, возможно, другие интерфейсы.

Схема веб-камеры приведена на рисунке 16.

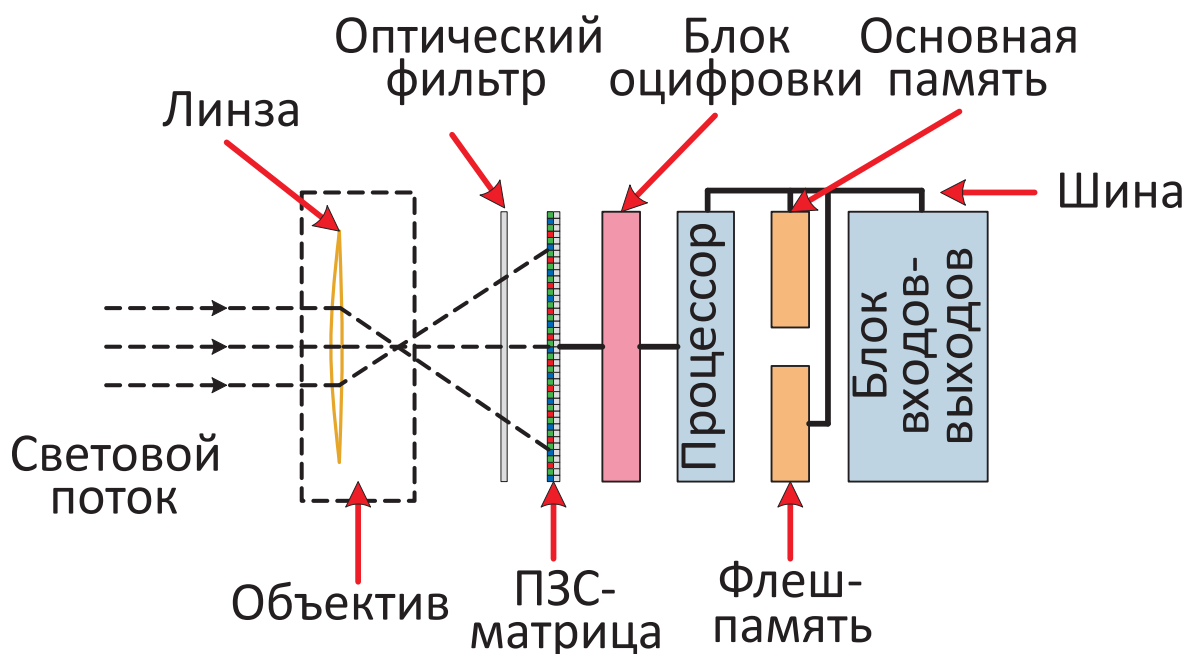


Рис. 16. Устройство цифровой камеры

Объектив веб-камеры, обычно сфокусирован на определённое расстояние съёмки, которое нельзя изменить (фикс-фокус). Объектив представляет собой систему линз (возможно с некоторыми дополнительными элементами), которая собирает отраженный от объекта съёмки свет и формирует изображение на матрице светочувствительных элементов. Многие технические характеристики веб-камеры, такие как фокусное расстояние, уровень и характер оптических искажений, разрешающая способность, зависят от объектива камеры.

Оптические фильтры имеют вид плоских параллельных пластинок и предназначены для обеспечения качественной цветопередачи, корректировки цвета, изменения яркости и контрастности фотографируемых объектов.

В отличие от аналоговых («пленочных») фотоаппаратов или камер, в которых носителем изображения выступала фотопленка, в цифровой веб-камере носителем изображения является матрица светочувствительных элементов — фотодиодов. Матрица может быть выполнена на основе различных технологий, из которых мы коротко рассмотрим только технологию приборов с зарядовой связью (ПЗС, Charge-Coupled Devices, CCD).

При попадании света из объектива на ПЗС-элемент матрицы в нем формируется электрический заряд, который затем «считывается» и преобразуется блоком оцифровки в натуральное число. Один ПЗС-элемент дает, таким образом, ровно одно натуральное число.

Для формирования цветных изображений ПЗС-элементы объединяются в группы из четырех элементов. Поверх группы размещается фильтр Байера (Bayer filter), который делает один ПЗС-элемент чувствительным к красному цвету, другой — к синему, а два оставшихся — к зеленому. Фильтр Байера можно представлять в виде квадратной пленки, разделенной на 4 равных квадрата, из которых один синий, один красный и два зеленых. Наличие двух зеленых фильтров объясняется особенностями человеческого световосприятия.

При включении камеры специальный контроллер определяет количество света, попадающего на матрицу, и проводит балансировку белого. Балансировка белого позволяет скорректировать цвета изображения, чтобы привести их к цветам, наблюдаемым человеком в естественных условиях (или до требуемых цветов). После этого изображение считывается с ПЗС-матрицы и сохраняется во встроенной оперативной памяти камеры. Далее изображение или группа изображений сжимается с целью сокращения занимаемого ими объема памяти, при этом мелкие детали могут утрачиваться. Наиболее часто используемыми форматами сжатия изображений и видеопотока являются JPEG, MJPEG, MPEG, Wavelet.

После того как изображение обработано, оно может быть либо сохранено во флэш-память, либо передано на компьютер или сервер, к которому камера подключена непосредственно (с помощью одного из интерфейсов, например, USB) или посредством вычислительной сети.

#### 4.3.8. Микрофоны

В этом разделе мы кратко рассмотрим принципы работы и основные характеристики микрофонов для компьютеров.

**Определение 4.16.** *Микрофоны для компьютеров — это устройства ввода информации, преобразующие акустические (звуковые) волны в электрические импульсы.*

На настоящий момент наиболее распространены динамические, конденсаторные и электретные микрофоны для компьютеров. Принцип действия электретного микрофона близок к конденсаторному, поэтому мы сосредоточимся только на двух первых видах.

#### 4.3.9. Динамические (катушечные) микрофоны

Схема динамического микрофона приведена на рисунке 17.

Важным элементом каждого микрофона является мембрана — элемент, способный совершать упругие колебания под воздействием акустической (звуковой) волны. В динамических микрофонах мембрана соединяется с катушкой индуктивности, помещенной в магнитное поле, создаваемое постоянным магнитом. Звуковая волна заставляет мембрану колебаться и тем самым приводит в движение проводник. При пересечении катушкой силовых линий магнитного поля в ней возникает ЭДС индукции, которую можно регистрировать, преобразовывать в электрический сигнал и передавать компьютеру.

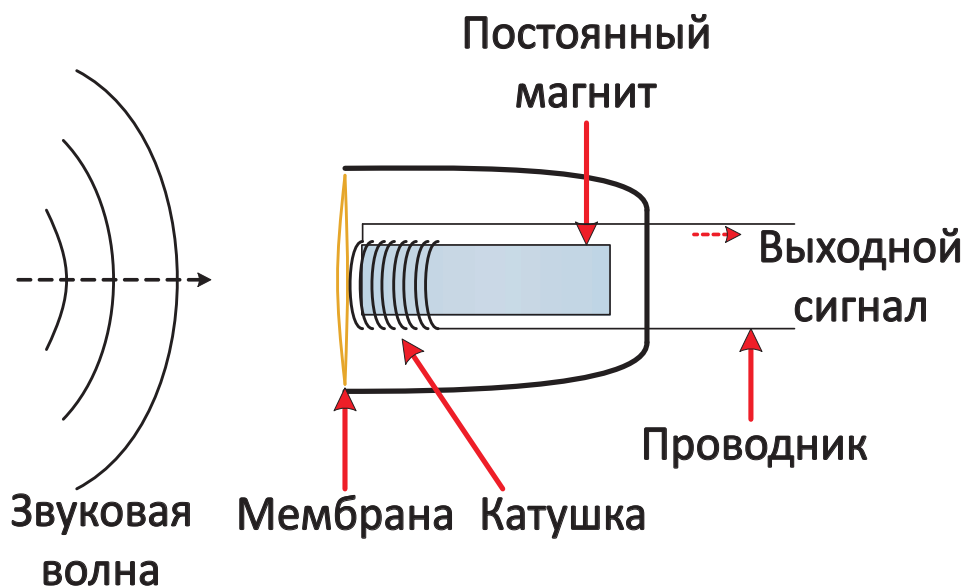


Рис. 17. Схема динамического микрофона

Недостатком динамического микрофона можно назвать его меньшую чувствительность по сравнению с конденсаторным микрофоном. Однако при этом динамический микрофон более стоек к внешним воздействиям (например, более устойчив к падениям и ударам), а также практически не зависит от погодных условий, что позволяет применять его вне помещений. Кроме того, динамические микрофоны способны выдерживать очень большое звуковое давление, что позволяет их использовать в экстремальных условиях.

#### 4.3.10. Конденсаторные микрофоны

Как следует из названия, основным элементом конденсаторного микрофона является конденсатор, одна из обкладок которого является мембраной. Поскольку емкость конденсатора зависит от расстояния между обкладками, то колебания мембраны под воздействием звуковой волны изменяют ёмкость конденсатора. Зарегистрированные изменения емкости служат основой для формирования полезных электрических сигналов.

Схема конденсаторного микрофона приведена на рисунке 18.

Конденсаторные микрофоны более чувствительны к звуковым волнам (так как процесс изменения емкости конденсатора более «тонкий», чем изменение ЭДС индуктивности в катушке при ее перемещении в магнитном поле). Поэтому, с одной стороны, они способны обеспечить лучшее качество звука, но, с другой стороны, они при этом воспринимают существенно больше «посторонних» звуков. Поэтому их широко применяют в студиях звукозаписи, где можно обеспечить отсутствие посторонних шумов.

К недостаткам конденсаторных микрофонов также относятся: относительно высокая стоимость, необходимость во внешнем питании, зависимость от погодных условий (например, уровня влажности и температуры и амплитуды их колебаний), относительная хрупкость, что также ограничивает область применения этих микрофонов.



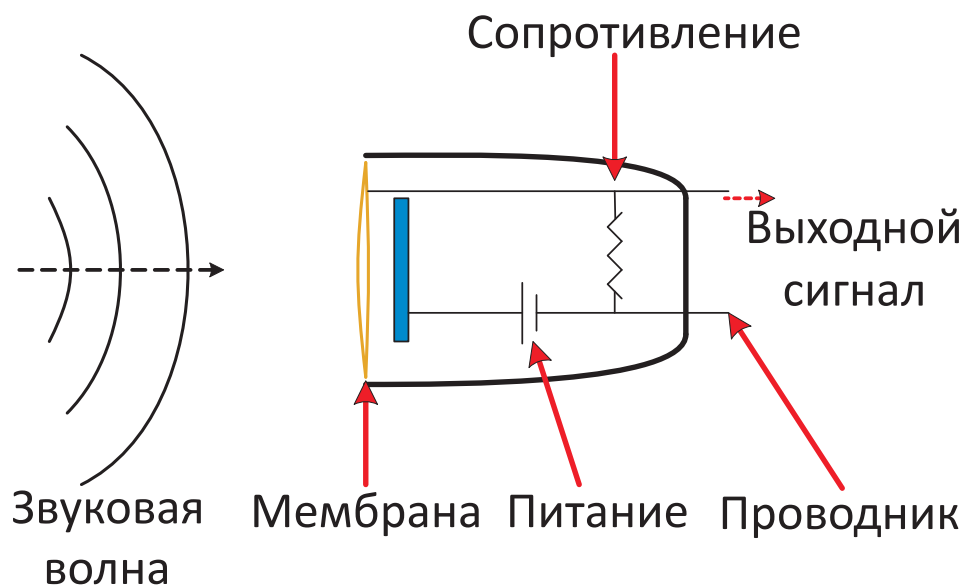


Рис. 18. Схема конденсаторного микрофона

#### 4.4. Вопросы и задания

4.1. Для чего предназначены процессор, оперативная память и устройства ввода-вывода компьютера?

4.2. Предположим, что мы используем 10 бит для адресации ячеек памяти размером 4 байта. Адресацию какого объема памяти мы сможем обеспечить?

4.3. Расположите в порядке увеличения объема памяти: (1) Страница. (2) Бит. (3) Слово. (4) Банк. (5) Ячейка.

4.4. Расположите виды памяти в порядке увеличения скорости работы. (1) Регистры процессора. (2) Твердотельные накопители. (3) Основная (оперативная) память. (4) Оптические диски. (5) Магнитные жесткие диски. (6) Кэш-память.

4.5. Какая концепция обычно реализуется в процессорах видеокарт?

1. Множественный поток команд, множественный поток данных.
2. Одиночный поток команд, множественный поток данных.
3. Множественный поток команд, одиночный поток данных.
4. Одиночный поток команд, одиночный поток данных.

4.6. Опишите принцип работы современного магнитного жесткого диска.

4.7. Какая шина наиболее распространена на текущий момент в персональных компьютерах?

4.8. Пусть тактовая частота шины компьютера составляет 10 ГГц. За один такт по шине можно передать 8 бит. Оцените скорость передачи информации по шине?

4.9. Опишите основные свойства проекционно-емкостных сенсорных экранов.

**4.10.** Перечислите элементы жидкокристаллического монитора и опишите принцип его работы.

**4.11.** Перечислите основные элементы лазерного принтера и опишите принцип его работы.

**4.12.** Перечислите элементы цифровой веб-камеры и опишите принцип ее работы.

**4.13.** Сравните динамический и конденсаторный микрофоны. Какими преимуществами и недостатками они обладают (по отношению друг друга)?

## 5. Основы операционных систем

### 5.1. Введение

Автоматизированная обработка информации в современном мире чаще всего происходит с использованием какой-либо **операционной системы** (далее **ОС**). Если какая-то информация и обрабатывается автоматизированно без применения распространенных ОС, то это скорее всего связано с применением какого-либо простого или специфического оборудования, на которое просто не устанавливается ОС, но на котором работает какая-то встроенная программа. Скажем, водонагреватель или стиральная машина — никаких ОС там нет, но они автоматизированно обрабатывают информацию. Но в наступающий век интернета вещей уже существуют домашние устройства, работающие на широко распространенных ОС или их ответвлениях (вероятно, даже водонагреватели и стиральные машины). По всей видимости, никого уже не удивит телевизор на Android, но вот холодильником на Linux, думаю, можно. Однако такой уже существует в продукции компании Samsung и работает он на производной от Linux мобильной операционной системе Tizen.

Таким образом, мы живем в мире, в котором персональные данные, конфиденциальная информация, государственная тайна и другая чувствительная к раскрытию информация часто обрабатывается на одной из распространенных операционных систем: Windows, Windows Server, MacOS, iOS, производные Linux, среди которых Android, Ubuntu, CentOS, Debian, Red Hat и т. д. Кроме десктопных<sup>3</sup>, мобильных и серверных ОС информация также проходит через множество сетевого оборудования, на котором работают свои ОС, например, под управлением проприетарной Cisco Internetwork Operating System работают многие маршрутизаторы и коммутаторы Cisco, под управлением производной от Linux ОС работают фаерволы Cisco PIX, Cisco ASA, сетевое оборудование производителя Juniper работает под управлением производной от Linux ОС Junos OS, более того, под управлением производных от Linux ОС работают российские криптошлюзы ViPNet HW, а также фаерволы Рубикон и т. д.

Во всех «точках» обработки информации: на мобильных телефонах, на ПК, на сетевом оборудовании, на серверах — существуют свои пути нелегитимного доступа к информации, а из-за широкой распространенности довольно узкого круга ОС методы атак зачастую похожи друг на друга.

### 5.2. Определение операционной системы

Выше уже довольно много раз упоминалось словосочетание «операционная система». Настало время немного формализовать это понятие.

Под ОС понимают программное обеспечение, которое

1. предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных (для программистов) абстракций<sup>4</sup> и

---

<sup>3</sup>Десктопными (от англ. desktop) или настольными называют ОС, которые чаще всего устанавливаются на персональные компьютеры, например, Windows 7, Windows 8.1, Windows 10, Ubuntu, MacOS и т. д.

<sup>4</sup>Под абстракциями ОС понимаются некоторые механизмы ОС, которые предоставляются другому программному обеспечению для выполнения его функций. Проведем параллель: переменная в языке программирования — это абстракция, под которой в конкретный момент времени может пониматься

2. управляет этим аппаратным обеспечением.

Разберем каждый из этих двух аспектов подробнее.

### 5.2.1. ОС как провайдер ресурсов

Для понимания этого аспекта ОС распишем по пунктам примерный список ресурсов, которые нужны любому приложению, чтобы выполняться, и то, что реализовано в ОС для предоставления этого ресурса:

1. **Процессорное время.** Приложение требует процессорное время для выполнения своего кода.

Современные ОС должны обеспечивать возможность одновременного выполнения многих приложений на компьютерах с разным количеством ядер процессора, в том числе на одноядерных процессорах. Поэтому во всех ОС присутствует такой компонент, как **планировщик**, который занимается предоставлением процессорного времени приложениям. Каждому приложению планировщик дает какое-то небольшое количество времени (несколько миллисекунд) на выполнение своего кода. Когда время заканчивается, ОС прерывает выполнение приложения и передает управление планировщику. Планировщик решает, какое приложение следующим получит процессорное время и запускает его выполнение. Таким образом, в ОС может псевдопараллельно работать множество приложений: процессор просто очень быстро переключается и выполняет понемногу каждое приложение, что создает впечатление их одновременной работы (смотри рисунок 19).

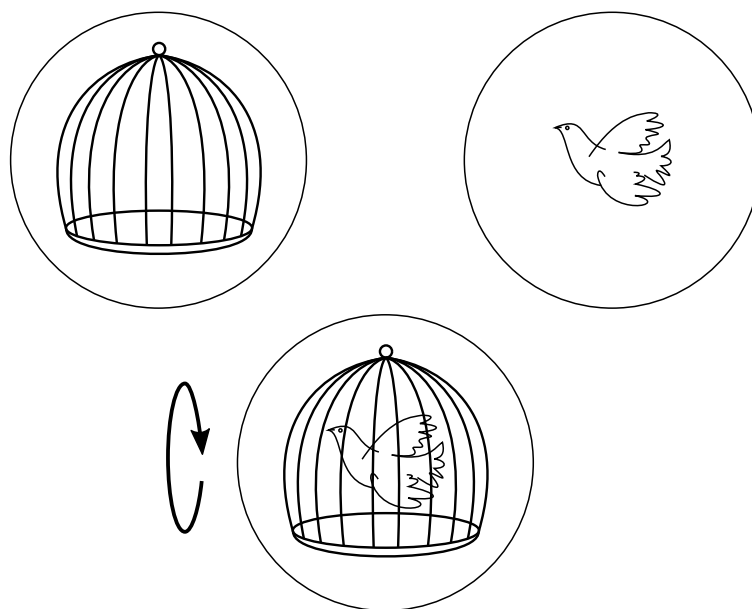


Рис. 19. Псевдопараллельное выполнение приложений в ОС. Круговая стрелка показывает быструю смену картинок (выполняющихся на процессоре приложений)

---

значение в регистре процессора, адрес ячейки оперативной памяти, объект какой-то сложной структуры в программе и т. д.

2. **Память**<sup>5</sup>. Приложению необходима оперативная память для размещения в ней своего кода и данных.

ОС должна разделить между всеми приложениями оперативную память. Эту задачу решает подсистема управления памятью. Она реализует функции выделения и освобождения памяти, увеличения и уменьшения выделенной части памяти, блокировки памяти от выгрузки на внешний носитель, отображения файлов в память и т. д.

3. **Устройства ввода/вывода**. Приложению обычно требуются устройства для предоставления входной информации и вывода результата его работы. Такими устройствами могут быть монитор, клавиатура, мышь, жесткий диск, сетевая карта и т. д. Для предоставления этих ресурсов ОС реализует множество абстракций.

Для доступа к сети ОС предоставляет приложениям **сокеты**, через которые можно отправить и принять информацию из сети по стеку протоколов TCP/IP (смотри рисунок 20 (a)).

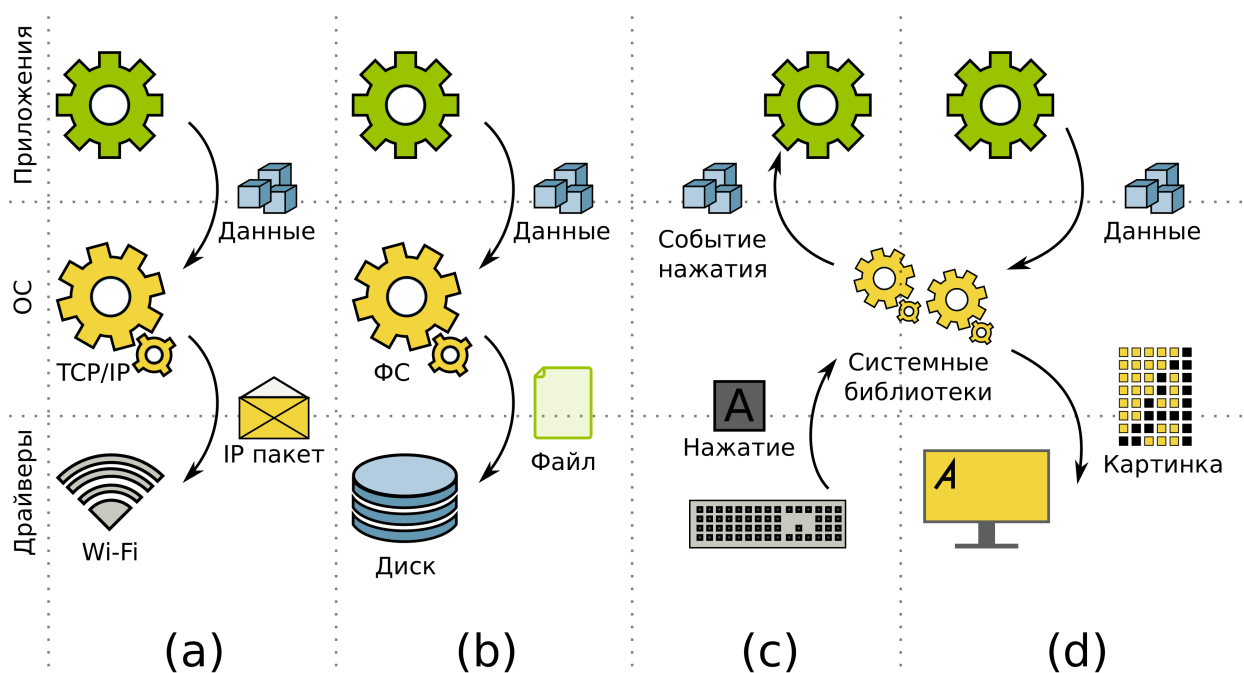


Рис. 20. ОС предоставляет ресурсы компьютера приложениям в виде удобных абстракций

<sup>5</sup>Здесь и далее под памятью понимается именно оперативная память (память с произвольным доступом, RAM). Это быстрая энергозависимая память, в которой приложения хранят свои код и данные, необходимые во время выполнения. Оперативная память не может хранить данные, когда она обесточена. Когда речь будет идти про память жесткого диска, твердотельного накопителя, флеш-память, то будут использоваться слова «диск» или «внешний носитель».

Доступ к жесткому диску чаще всего идет через одну из поддерживаемых ОС **файловых систем**. С помощью реализации файловой системы ОС предоставляет приложениям абстракцию **файла** (смотри рисунок 20 (b)), разграничивает доступ к файлам между пользователями ОС, восстанавливает данные на внешнем носителе после аварийного завершения работы, ведет аудит доступа к файлам и т. д.

Одним из самых простых способов получения доступа к клавиатуре и дисплею в ОС является написание консольных приложений: ОС предоставляет приложениям набор библиотек для создания таких приложений<sup>6</sup>. Пользователь работает с такой программой, вводя текстовые команды и получая результат в текстовом виде на экране монитора. Для программиста написание таких приложений — очень простое дело: с помощью функций «считай с консоли» программист запрашивает у пользователя данные, затем сохраняет введенные данные в переменные, вычисляет некоторый результат, зависящий от этих переменных, и вызывает функцию «напиши на консоль» для вывода результата. Создание окна для ввода и вывода в него информации, передача только тех нажатий на клавиатуру, которые были сделаны, когда это окно было активным, непосредственная отрисовка символов какого-то шрифта в этом окне, — все эти задачи решает ОС незаметно для программиста (смотри рисунок 20 (c, d)).

### 5.2.2. ОС как менеджер ресурсов

В предыдущем пункте было сказано достаточно на текущий момент о том, как планировщик управляет процессорным временем, поэтому здесь на этом останавливаться не будем.

Относительно подсистемы управления памятью выше были выделены некоторые моменты, которые видны со стороны приложения, как пользователя оперативной памяти. Но многие вещи подсистема управления памятью делает скрытно от приложений. Перечислим некоторые из них:

1. ОС обеспечивает безопасность памяти. Вот неполный список вещей, которые делает ОС:
  - а) ОС защищает свою память от записи со стороны пользовательских приложений (смотри подраздел 5.3.6).
  - б) Каждое приложение имеет свою память, защищенную от доступа со стороны других приложений.
  - в) ОС предоставляет возможность создавать и создает сама участки памяти, в которых не может быть исполняемого кода приложения. Это необходимо для предотвращения записи и исполнения произвольного кода злоумышленником в памяти.
  - г) В разных ОС есть механизмы, которые не разрешают какой бы то ни было доступ в память пользовательских приложений во время выполнения кода самой ОС. Это опять же защита от потенциальных атак, в

---

<sup>6</sup>Библиотека — подключаемый к программе модуль, который расширяет функционал программы. Системная библиотека — библиотека, которая поставляется как составная часть ОС. Использование библиотек выгодно тем, что программы могут брать какой-то общий функционал из них, а не реализовывать в каждой программе.

которых злоумышленник записывает зловредный код в контролируемую им память, а затем как-то передает на нее управление из кода ОС (смотри подразделы 5.3.1, 5.3.6).

2. Если разные приложения используют в своей работе одни и те же библиотеки, то ОС может экономить память за счет загрузки в реальную память одной копии этой библиотеки и отображения<sup>7</sup> ее в память всех приложений.

Если какое-то из таких приложений изменит часть данных в библиотеке в процессе своего выполнения, то будет скопирована отдельно только изменившаяся часть. Таким образом, приложения видят общую неизмененную часть библиотеки, которая присутствует в памяти в единственном экземпляре, а также свои измененные части, которые отображаются в память каждого приложения отдельно от других.

3. ОС управляет выгрузкой части оперативной памяти на жесткий диск.

Часто приложения запрашивают большое количество памяти, чтобы ее хватило в ходе выполнения приложения во всех сценариях. Однако не вся память используется одновременно. Приложение обычно в небольшой интервал времени использует небольшой объем своей памяти. Это означает, что можно держать в памяти только те данные, которые приложения активно используют сейчас. Такой подход в теории позволяет выполнять больше приложений с небольшими временными затратами на выгрузку ненужных частей на диск.

Осталось поговорить об устройствах ввода/вывода информации. В ОС работой с этими устройствами занимается подсистема ввода-вывода ОС. Работа этой подсистемы опирается на драйверы устройств и части ОС, связанной с низкоуровневым доступом к аппаратному обеспечению, так называемому *уровню абстракции оборудования* (от англ. hardware abstraction level, HAL). Драйверы обеспечивают работу конкретного оборудования и опираются на HAL, которая абстрагирует драйвер от особенностей платформы, на которой он работает. HAL предоставляет драйверам функции чтения и записи относительно некоторых абстракций, через которые идет управление устройствами и обмен данными с ними.

Перечислим возможности, которые обеспечивает эта часть ОС для лучшего ее понимания:

1. Код драйвера устройства может быть написан в отвлечении от архитектуры компьютера, что делает его легко переносимым.
2. ОС позволяет встраивать драйверы в цепочки для добавления дополнительного функционала.

Например, драйвер антивирусного обеспечения может быть встроен перед драйвером файловой системы (смотри пункт 3) для проверки данных, записываемых на диск.

Встраивание нового драйвера в цепочку драйверов устройства может использоваться и зловредными приложениями. Так, приложение, перехватывающее символы, введенные с клавиатуры, может встраивать промежуточный драйвер в цепочку драйверов клавиатуры.

---

<sup>7</sup>Понятие отображения памяти приложений на физическую память связано с виртуальной памятью и раскрывается в 5.3.6.

3. ОС может реализовать некоторые удобные абстракции с помощью своих драйверов, которые будут работать над драйверами конкретных устройств.

Так, над драйвером шины SATA, по которой производится передача данных между процессором (основной памятью) и жестким диском, в ОС может работать множество других драйверов, в частности, драйвер файловой системы (ФС). В Windows это драйвер NTFS, в Linux, например, Ext4, а в MacOS — APFS. То есть, работая в ОС, не нужно заботиться об общении с контроллером жесткого диска по шине SATA, вместо этого вся работа ведется с высокоуровневой абстракцией «контейнера для хранения данных» — файлом.

Еще одним примером может быть драйвер сетевого стека TCP/IP, которым опосредованно пользуются большинство сетевых приложений. Программисту не нужно знать все тонкости сетевых протоколов и реализовывать их в своем приложении. Достаточно использовать абстракцию ОС сокет и операции над ним.

4. ОС позволяет на лету подключить и удалить устройство из системы, а также автоматически распознать новое устройство, подключенное к компьютеру в выключенном состоянии, и инициализировать его работу, или же предложить пользователю настроить устройство, если его драйвер не был найден ОС. Эта функция известна как **Plug and Play (PnP)**.
5. ОС управляет питанием устройств. Выключает некоторые из них или переводит их в режим пониженного потребления энергии, когда они не используются, а также когда компьютер переходит в спящий режим или режим гибернации<sup>8</sup>.
6. ОС обеспечивает безопасность операций ввода-вывода. Например, ОС запрещает запись в определенный файл пользователю, у которого нет на это прав, а также запрещает писать байты данных напрямую на диск в то место, где расположен такой файл. Также ОС не позволяет пользовательским приложениям «просто так» прослушивать все вводимые с клавиатуры символы или идущий через сетевую карту трафик. И так далее.

Также ОС может обеспечивать свою безопасность посредством проверки электронной подписи доверенного разработчика на файле драйвера устройства перед тем, как загрузить его код в память.

### 5.3. Основные понятия операционной системы

#### 5.3.1. Режим ядра и режим пользователя

Современные ОС используют аппаратно поддерживаемую иерархическую систему защиты своего кода и данных для повышения отказоустойчивости. Этот механизм называется **кольцами защиты** и реализован в большинстве современных процессоров. Обычно используется два кольца, хотя некоторые архитектуры реализуют четыре. Эти кольца обычно называют **режимом ядра** (или **супервизора**) и **режимом пользователя**. Различия между режимами состоят в основном в следующем:

---

<sup>8</sup>В спящем режиме обесточивается почти все аппаратное обеспечение компьютера, но не обесточивается оперативная память. Она хранит информацию о исполняемых в ОС приложениях на момент ухода в спящий режим. В режиме гибернации обесточивается весь компьютер, при этом содержимое оперативной памяти записывается на внешний носитель. При следующем запуске ОС обнаружит, что до этого она ушла в гибернацию и восстановит содержимое оперативной памяти (читай восстановит свою работу) с внешнего носителя.



- В режиме ядра доступны все инструкции процессора, в режиме пользователя только непривилегированные. Например, инструкция запрета прерываний является привилегированной и ее нельзя исполнить в режиме пользователя, так как это сделало бы невозможной работу планировщика (смотри 5.3.5).
- В режиме ядра исполняемый код может получить доступ ко всей памяти, в режиме пользователя код работает только с памятью текущего приложения, которую ОС выделила ему.

Из пунктов выше становится понятно, как ОС защищает себя через механизм колец защиты: код приложений работает в режиме пользователя. Таким образом, приложение не может выполнить потенциально опасные инструкции процессора и имеет доступ на изменение только к своей памяти, что является хорошим способом защиты от ошибок в приложениях, которые могут привести к аварийному завершению работы ОС, а также от намеренного вмешательства со стороны приложений в работу внутренних механизмов ОС. Код самой ОС работает в режиме ядра, что дает ОС всю полноту действий<sup>9</sup>.

Два следующих пункта дадут лучшее понимание того, как процессор меняет уровни защиты во время работы.

### 5.3.2. Прерывания

**Прерывания** — механизм процессора для обработки событий, которые требуют немедленной обработки со стороны программного обеспечения. Прерывания делятся на два типа:

1. *Аппаратные прерывания.* Используются устройства компьютера для информирования ОС о событиях, связанных с ними, на которые нужна реакция со стороны ОС. Физически это электрические сигналы, поступающие в процессор от устройства. Например, нажатие на клавишу клавиатуры или движение мышкой приводит к передаче сигнала в процессор, а процессор при этом передает управление части ОС, отвечающей за эти события. ОС считает нажатую клавишу или позицию мыши и передаст эту информацию дальше запущенным приложениям.
2. *Программные прерывания.* Возникают, когда произошла ошибка выполнения очередной инструкции процессора или когда была исполнена специальная инструкция, инициирующая такое прерывание. Например, в случае деления на ноль, процессор сообщит ОС о программном прерывании, так как он не может выполнить эту инструкцию.

При возникновении прерывания процессор приостанавливает исполнение текущего приложения, сохраняет его состояние для того, чтобы потом его возобновить, и передает управление в специальный обработчик прерывания, заданный ОС. При этом процессор переходит из режима пользователя в режим ядра, так как код обработчика прерывания

---

<sup>9</sup>В современных ОС часто встречается ситуация, когда часть программного кода ОС также исполняется в режиме пользователя. Это сделано также для отказоустойчивости и безопасности. Например, драйверы устройств можно запустить в режиме пользователя. В таком случае возникшую в драйвере ошибку можно будет обработать на уровне ОС и, скажем, перезагрузить драйвер или просто выключить устройство. Это не приведет к аварийному выключению компьютера, как было бы с драйвером, работающем в режиме ядра.

находится в ядре. После обработки прерывания выполнение приложения может быть возобновлено сразу же, в другой отрезок времени, или ОС может завершить выполнение приложения из-за возникшего прерывания.

### 5.3.3. Системные вызовы

Как говорилось ранее, одной из функций ОС является предоставление ресурсов компьютера для приложений. Для работы с ресурсами компьютера ОС предоставляет приложениям набор функций, которые называются системными вызовами. Чтобы выполнить системный вызов, нужно исполнить специальную инструкцию процессора, которая переведет процессор в режим ядра и исполнит обработчик этого системного вызова. Приведем примеры системных вызовов по группам их назначения:

1. Управление процессами: создание, завершение процессов и потоков, загрузка библиотек, функции ожидания, функции синхронизации между процессами и потоками, выделение и освобождение памяти и т. д.
2. Управление файлами: создание и удаление файлов, операции с файлами и атрибутами файлов и т. д.
3. Управление устройствами: создание и удаление устройств, операции с ними и т. д.
4. Управление сетью: создание и удаление сетевых подключений и функции передачи данных и т. д.
5. Управление безопасностью: изменение параметров доступа к объектам, проверка возможности доступа, изменение текущих параметров доступа процесса или потока и т. д.

### 5.3.4. Приложения, процессы, потоки

Выше специально не упоминались понятия «процесс» и «поток». Вместо этого всегда писалось «приложение». Это было сделано намеренно, так как слово «приложение» интуитивно понятно, но слова «процесс» и «поток» требуют более формального подхода, так как являются довольно точными понятиями ОС.

Давайте для начала разберемся со словом «приложение». Приложение — это не что иное, как набор файлов. Некоторые файлы являются исполняемыми, то есть их код будет загружен в оперативную память и получит процессорное время для выполнения. Некоторые файлы — это ресурсы, которые использует приложение в своей работе. Они или их части могут загружаться и выгружаться из оперативной памяти в ходе выполнения приложения. «Приложения» еще часто называют «программами». Сегодня можно встретить множество разнообразных приложений, работающих в ОС. Есть те, которые преобразованы в машинные команды процессора и чей код готов к загрузке в оперативную память и выполнению, а есть те, чей код переводится в команды процессора на лету промежуточным приложением. Есть те, которые требуют установки, а есть те, которые не требуют, или вообще работают из браузера. Есть графические приложения, есть приложения без интерфейса, есть и такие, которые лишь обслуживают другие приложения, например, базы данных или криптопровайдеры. Последние называются *сервисами*<sup>10</sup>.

---

<sup>10</sup>Сервисы (или демоны в Linux) — приложения, работающие в фоне и предоставляющие какие-то функции другим приложениям.

Теперь переходим к понятию процесса. **Процессом** в ОС называют экземпляр запущенного приложения. Пока приложение еще не запущено, а просто лежит на жестком диске, это просто приложение, а не процесс. Процесс появляется в результате запуска приложения. Приложения обычно запускаются по одной из следующих причин:

1. Это важное для работы ОС приложение, и оно запускается автоматически в ходе запуска самой ОС. Простым примером здесь может быть приложение winlogon на Windows, в котором пользователь вводит свои имя и пароль для входа в систему и которое пользователь видит после блокировки компьютера.
2. Это приложение-сервис, которое настроило свой автоматический запуск при старте системы.
3. Это приложение из автозапуска. *Автозапуск* — функция, позволяющая каждому пользователю ОС запустить какие-то свои приложения при старте системы.
4. Это приложение, запущенное планировщиком.
5. Приложение запустил сам пользователь.
6. Приложение запустило другое приложение.

Фактически процесс представляет собой набор необходимых для работы приложения данных, которые ОС содержит в оперативной памяти.

Теперь о потоках. Если процесс — это экземпляр запущенного приложения, то **потоком** можно назвать экземпляр конкретной ветви исполнения приложения. В современных ОС у процесса всегда есть хотя бы один поток. Это поток, который создается при старте приложения и который служит для выполнения главной функции приложения. В дальнейшем процесс может создать более одного потока. Сейчас потоки применяются почти в любом приложении, так как они повышают производительность приложений. Вот некоторые преимущества потоков перед процессами относительно эффективности:

1. Планировщик современных ОС выдает процессорное время именно потокам. Здесь важно то, что планировщик может выбрать несколько потоков одного процесса для выполнения в следующий отрезок времени. Таким образом, процессор может одновременно выполнять несколько потоков одного процесса, что значительно увеличивает производительность приложения в этот отрезок времени.
2. Если один из потоков процесса заблокировался на выполнении какой-то длительной операции (обычно ожидание ввода пользователя или чтение или запись данных на жесткий диск), планировщик может тут же выдать время другому потоку процесса. То есть не весь процесс ждет завершения какой-то долгой операции, а только один поток.
3. Создание нового потока в ОС происходит гораздо быстрее, чем создание нового процесса. Таким образом, приложения, которые склонны запускать дочерние процессы для решения своих задач, могут сильно увеличить свою производительность, если будут создавать потоки с аналогичным функционалом ради этого.

4. Межпотокное взаимодействие быстрее межпроцессорного, так как потоки разделяют между собой общую память процесса. Один поток может изменять значение переменной в памяти процесса, а другой считывать изменившуюся переменную. Между процессами такое организовать сложнее, так как память одного процесса защищена от прямого доступа со стороны другого процесса. Для этой цели в ОС реализуются специальные механизмы межпроцессорного взаимодействия.

Перейдем к описанию жизненного цикла процесса. Все начинается с того, что процесс запускается, при этом создается и запускается поток, который исполняет главную функцию приложения. Далее процесс существует в системе, пока у него есть хотя бы один активный поток. Потоки в свою очередь работают по схеме, изображенной на рисунке 21. Рассмотрим состояния потока:

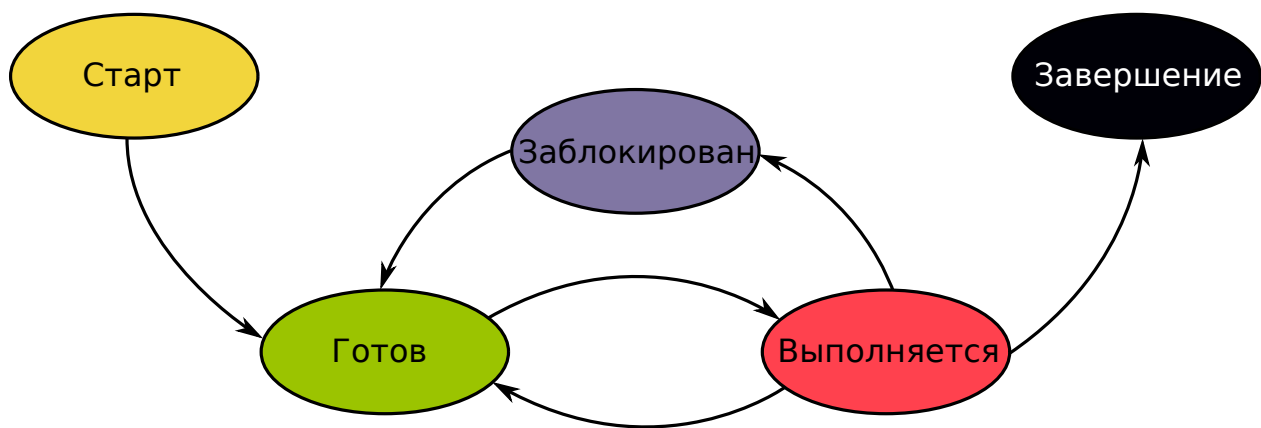


Рис. 21. Схема состояний и переходов потоков

1. **Старт.** В этом состоянии поток находится после создания, пока отработывают функции ОС, обеспечивающие его дальнейшую работу.
2. **Готов.** В состоянии готовности поток находится всегда, когда он готов к выполнению на процессоре. То есть ему ничего не мешает приступить к исполнению следующей инструкции программы.
3. **Выполняется.** В этом состоянии поток находится в момент исполнения на процессоре.
4. **Заблокирован.** В этом состоянии поток находится, когда он ожидает завершения какой-либо операции. Обычно это операция, связанная с устройствами ввода-вывода: открытие файла, прием данных по сети, ожидание ввода с клавиатуры и т. д. Но бывают и другие примеры, например, поток может войти в состояние блокировки намеренно при работе нескольких потоков с одной ячейкой памяти: если в ячейку памяти идет запись другим потоком, то текущий поток блокируется и ждет завершения операции, когда другой поток закончит свою операцию, можно будет продолжить работу с ячейкой памяти.
5. **Завершение.** В этом состоянии поток находится при завершении своей работы, пока отработывают функции ОС, обеспечивающие его корректное завершение.

Теперь о переходах между состояниями. Все начинается с состояния «Старт», в котором происходит инициализация потока. После завершения всей подготовительной работы ОС переводит поток в состояние «Готов»: поток только что был создан и ничто не мешает ему выполнить свою первую инструкцию. Далее поток ожидает, пока планировщик не выдаст ему квант времени для выполнения на процессоре. Когда это происходит, ОС переводит поток в состояние «Выполняется», и поток начинает свою работу на одном из процессоров компьютера. Далее могут быть три ситуации:

1. Поток возвращается в состояние «Готов». Чаще всего это происходит, когда у потока завершился квант времени.
2. Поток переходит в состояние «Заблокирован». В общем случае это происходит потому, что поток хочет осуществить доступ к какому-то ресурсу, который либо занят сейчас, либо сама операция доступа к ресурсу ощутимо дольше кванта, выделяемого на выполнение потока. В таком случае нелогично оставлять процессор простаивать без работы, поэтому ОС прерывает выполнение потока, переводит его в состояние «Заблокирован» и переходит к планированию выполнения одного из потоков в состоянии «Готов».
3. Поток завершает свое выполнение, перейдя в состояние «Завершение». Это происходит, когда поток выполнил функцию приложения, которую ему нужно было выполнить изначально, или когда возникла ошибка и поток нужно аварийно завершить.

Из состояния «Заблокирован» в состояние «Готов» поток переходит, когда в ОС завершились действия по осуществлению доступа к ресурсу. Например, ОС считала строку текста из файла, и поток готов продолжить свою работу с новопрочитанной строкой.

### 5.3.5. Планировщик и смена контекста

Теперь, когда у нас есть базовая информация о прерываниях, процессах и потоках, хотелось бы дополнить информацию о планировщике. В следующих пунктах опишем основные свойства планировщика, характерные для большинства современных ОС:

- Планировщик, как правило, планирует выполнение потоков. То есть единицами планирования выступают именно потоки, а не процессы. Благодаря этому планировщик может выделить процессорное время нескольких ядер процессора на выполнение нескольких потоков одного процесса. Этим достигается истинный параллелизм, в отличие от псевдопараллелизма, иллюзия которого возникает при быстрой смене выполняющихся на процессоре процессов.
- Планировщик выдает потокам маленький отрезок времени на выполнение, называемый **квантом**. Квант может быть фиксированный по размеру, а может быть различным для различных потоков. Например, в Windows есть технология переменных квантов, благодаря которой каждый поток процесса, окно которого находится на переднем плане, получает квант втрое больше обычного.
- Как правило, в современных ОС потокам назначаются приоритеты и первую очередь выполнения получают потоки с наибольшим приоритетом.

- Планировщик планирует выполнение нового потока в одной из следующих ситуаций:
  - Когда поток только что был создан или вышел из состояния блокировки.
  - Когда закончился квант, выделенный для выполнения потока. Вообще возможность выделения потокам фиксированных отрезков времени предоставляет устройство — высокоточный таймер. Этот таймер с определенной периодичностью посылает прерывания в процессор. ОС обрабатывает это прерывание, передавая управление планировщику, который предоставляет процессорное время следующему потоку.
  - Когда поток вошел в состояние блокировки. Чаще всего происходит из-за выполнения операции ввода-вывода, что означает, что поток больше не может сделать ничего полезного на текущий момент, пока он не получит ответ на свою операцию.
  - Когда произошло прерывание. Прерывание от устройства компьютера может быть, например, сигналом об окончании операции ввода-вывода, которую инициировал поток с большим приоритетом. В такой ситуации текущий поток может выполняться за неполный квант отведенного ему времени, пока его не заменит более приоритетный, ставший готовым к выполнению поток. Также прерывание может привести к аварийной остановке текущего процесса, и возникнет необходимость планировать поток другого процесса.
- Если нет потоков, готовых к выполнению, то работает поток специального процесса простоя системы.

Процесс смены исполняющегося потока называется **сменой контекста**. При смене контекста ОС сохраняет все необходимые для возобновления работы потока данные, фактически это некоторый набор регистров процессора, загружает данные другого потока и начинает его выполнение.

Рассмотрим пару простых идей, которые могут быть реализованы в планировщиках разных ОС. Первая идея — планирование «по круговой» (смотри рисунок 22). Суть данного планирования в следующем:

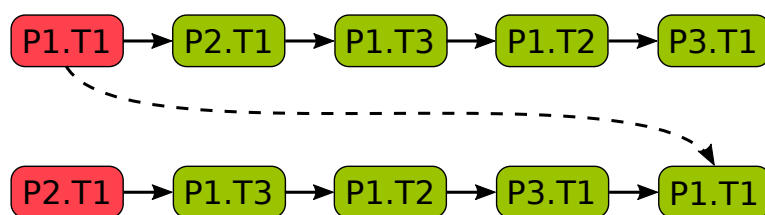


Рис. 22. Планирование «по круговой». Буквой Р обозначены процессы, буквой Т — потоки, Р1 — процесс в системе с номером 1, Р3.Т1 — поток с номером 1 процесса с номером 3. Выполняется первый поток в очереди — Р1.Т1. После завершения своего выполнения Р1.Т1 переходит в состояние готовности и встает в конец очереди. Следующим свое процессорное время получает поток Р2.Т1

- все потоки, готовые к выполнению, выстраиваются в очередь;

- процессорное время выдается первому в очереди потоку;
- когда поток выходит из состояния выполнения, то он либо попадает в конец очереди, в случае возврата в состояние готовности, либо покидает очередь;
- когда поток возвращается в состояние готовности из состояния блокировки, то он встает в конец очереди.

С помощью такого планирования, конечно, можно создать работающую ОС, но ее работа будет далека от желаемой. Проблема в том, что в таком планировании все потоки равны между собой и все получают примерно равное количество процессорного времени. Недостаток этого будет явным в десктопных или мобильных ОС, в которых важно, чтобы приложение, в котором пользователь работает непосредственно сейчас, обладало высоким откликом. Также в ОС существуют системные процессы, выполняющие важные для работы ОС функции, и код этих приложений целесообразно выполнять в первую очередь. Поэтому на сцену выходит планирование по приоритетам (смотри рисунок 23).

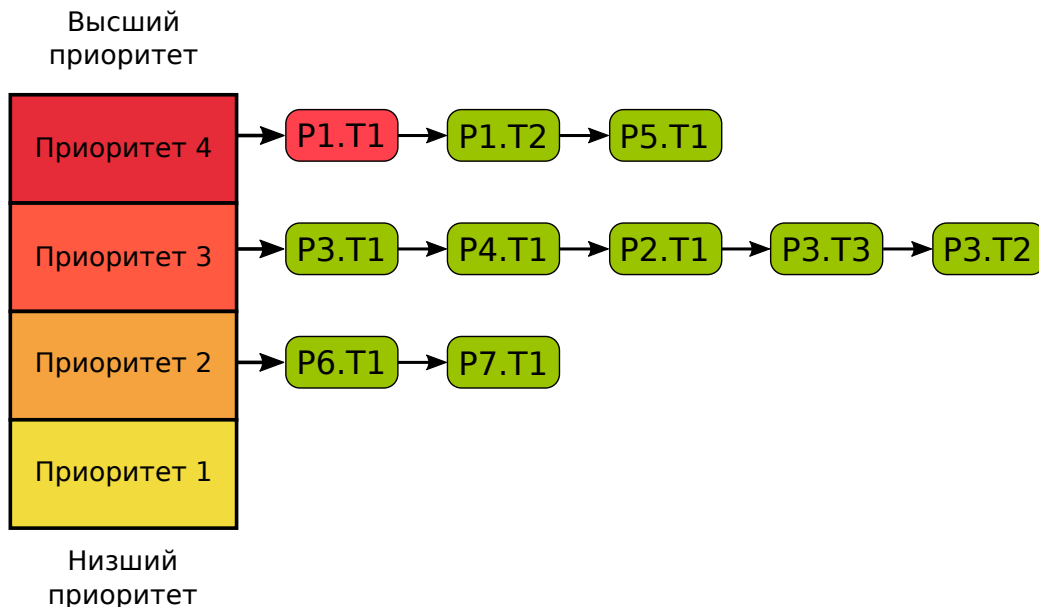


Рис. 23. Планирование по приоритетам. Обозначения как на рисунке 22. На каждом приоритете работает планирование по круговой. Первыми процессорное время получают потоки с наивысшим приоритетом

Планирование по приоритетам работает следующим образом:

- на каждом приоритете планировщик работает как при планировании по круговой;
- первыми планируются потоки из очереди с наивысшим приоритетом.

### 5.3.6. Управление памятью

Современные процессоры и ОС используют механизм **виртуальной памяти** для управления оперативной памятью компьютера. Чтобы понять идею виртуальной

памяти, нужно понимать, с какими трудностями в управлении памяти сталкивались инженеры и программисты по ходу развития компьютерных технологий.

Изначально память никак не управлялась и приложения могли напрямую обращаться к оперативной памяти. В таких условиях в ОС могло исполняться только одно приложение по следующей причине. Представим, что два приложения используют ячейку оперативной памяти с одним адресом: первое использует ее для хранения числа итераций цикла, а второе — просто как число. Представим, что оба приложения запущены одновременно. Если первое приложение уменьшит число итераций цикла, то изменится и число во втором приложении, что скорее всего приведет к ошибкам. Если второе приложение изменило число, то в первом могло выполниться неправильное число итераций цикла, что, опять же, ведет к ошибкам с большой вероятностью.

Поэтому необходимо было как-то разделить память процессов. Появилась идея **сегментной памяти**. Память каждого процесса отныне имела свой базовый адрес (начало) в оперативной памяти и размер. Начинаясь с базового адреса участок памяти указанного размера — сегмент. Сегменты процессов не пересекались и можно было запускать новые процессы, пока под их сегменты есть достаточно свободной памяти. Но у этого подхода была большая проблема — **внешняя фрагментация**.

Внешняя фрагментация состоит в том, что при продолжительном процессе запуска и завершения процессов в системе в памяти образуются свободные участки между сегментами текущих на данный момент приложений. В определенный момент времени можно получить ситуацию, что свободно очень много памяти, однако выделить один непрерывный сегмент памяти для работы даже маленького приложения уже нельзя. Чтобы исправить проблему, нужно запустить процесс **дефрагментации**. То есть сдвинуть все сегменты в одну сторону, чтобы с другой осталась только большая область свободной памяти. Но этот процесс является очень неэффективным. Поэтому была придумана другая идея организации памяти — виртуальная память.

Перечислим идеи, реализованные в виртуальной памяти, по пунктам:

1. Каждый процесс видит всю память как свою собственную, как будто в ней нет других процессов.
2. Процессы адресуют ячейки памяти виртуальными адресами. Эти адреса транслируются (отображаются) в реальные адреса с помощью таблиц трансляции. У каждого процесса эти таблицы свои. Поэтому два процесса могут использовать переменную по одному адресу, скажем, 200, но в первом процессе через таблицы первого же процесса 200 будет отображено в физический адрес, скажем, 300, а во втором через таблицы второго процесса 200 будет отображено в физический адрес, скажем, 100 (смотри рисунок 25).
3. Множества виртуальных адресов объединены в группы, называемые страницами. Множества физических адресов тоже. Страница — небольшой кусочек непрерывной памяти. Выделение памяти идет страницами. При этом странице в виртуальной памяти ставится в соответствие страница в физической. Несколько подряд идущих страниц в виртуальной памяти не обязательно идут подряд в физической.
4. Виртуальная память процесса делится на две части. Одну из частей использует сама ОС, и эта часть одинакова у всех процессов. Это нужно для того, чтобы после перехода процесса в режим ядра, код ОС, который отрабатывает в этом режиме, находился в одинаковом окружении вне зависимости от процесса. Проще говоря,



код чтения файла одинаков и у процесса блокнота, и у процесса графического редактора и находится он в части памяти ОС, которая одинакова у обоих процессов (смотри рисунки 24 и 25).



Рис. 24. Карта памяти процесса. В верхней части располагается код и данные ОС, в нижней код и данные процесса. Нижняя часть называется пользовательской, так как эта память отведена «пользователям» ОС — процессам. Пример изображен для архитектуры x64. В середине есть неотображенная на реальную память область адресов, так как архитектура x64 пока реализуется в компьютерах в усеченном виде, где есть ограничение по памяти 256 терабайт (ТБ): 128 для ОС и 128 для процесса. Адреса крайних страниц в памяти ОС и пользовательской (например, 00007FFF'FFFFFFFF) написаны в шестнадцатеричной системе счисления с разделением на группы по 8 цифр (символов)

### 5.3.7. Файловые системы

Файловые системы (ФС) являются очень важным компонентом ОС с точки зрения информационной безопасности, так как многие (если не все) охраняемые данные хранятся в ФС на каком-либо устройстве долговременного хранения. Дадим простое определение ФС.

**Файловая система** — механизм хранения данных в файлах, находящихся в иерархии директорий (каталогов).

В определении сразу видим два понятия: файлы и директории, о которых поговорим далее. Также видим, что ФС служит цели хранения данных. Для этого в ФС одного из подключенных к компьютеру внешнего носителя создают новый файл или открывают существующий и записывают туда необходимые данные. Записать данные в файл означает изменить содержимое файла. Отметим, что содержимое файлов в ФС хранится **кластерами** фиксированного размера. Кластеры в свою очередь делятся на сектора.

**Файлы** — некоторая абстракция, которая фактически представляет непосредственно сами данные и дополнительную информацию, необходимую для работы с данными в рамках ФС. Дополнительная информация может включать в себя имя файла, размер файла, дату последнего изменения, правила доступа к файлу и т. д.

**Директория** — специальный файл, содержимое которого разбито на одинаковые записи с информацией о лежащих внутри директории файлах.

В ФС можно выделить несколько категорий данных (смотри рисунок 26):

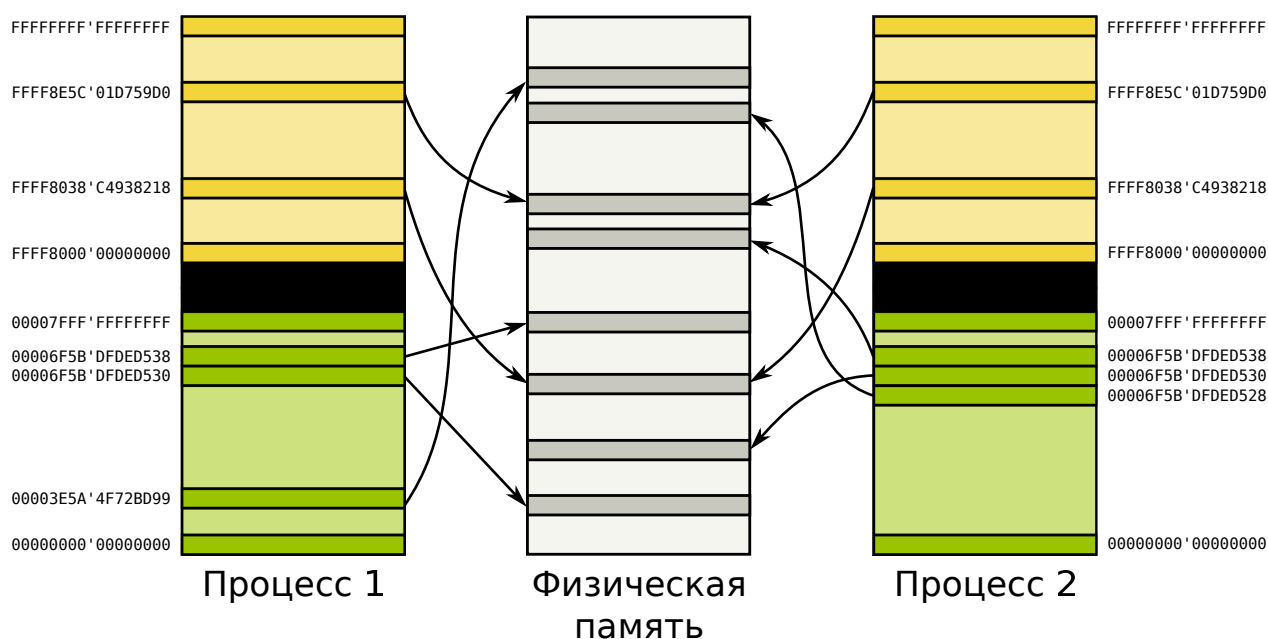


Рис. 25. Отображение виртуальных страниц на физические. Страницы по одинаковым виртуальным адресам в области ОС разных процессов отображаются на страницы по одинаковым адресам в физической памяти. Страницы же из пользовательских областей, расположенные по одинаковым виртуальным адресам, как правило, отображаются на разные страницы в физической памяти (исключение составляют разделяемые страницы)

#### 1. Базовые данные.

К этим данным, например, относятся размеры **сектора** и **кластера**. Содержимое файлов в ФС хранится кластерами фиксированного размера. Кластеры в свою очередь делятся на секторы.

Также к этим данным относится местоположение **корневой директории**, содержащей список файлов, хранимых в ФС. Относительно корневой директории адресуются все файлы ФС.

2. *Имена файлов.* Эти данные содержат информацию о именах файлов. Как правило, данные этой категории хранятся в каталогах, в записях которых содержатся адреса на метаданные файла.
3. *Метаданные* — это все данные файла, кроме непосредственно содержимого. Сюда входят временные метки, адреса кластеров содержимого, параметры безопасности и т. д.
4. *Содержимое файлов* — данные ФС, непосредственно относящиеся к содержимому файлов.
5. *Прикладные данные* — данные, обеспечивающие специальные возможности. Например, журналы ФС могут восстановить работу ФС после аварийного выключения компьютера, а квоты позволяют ограничить размер диска, доступный для использования указанными пользователями.

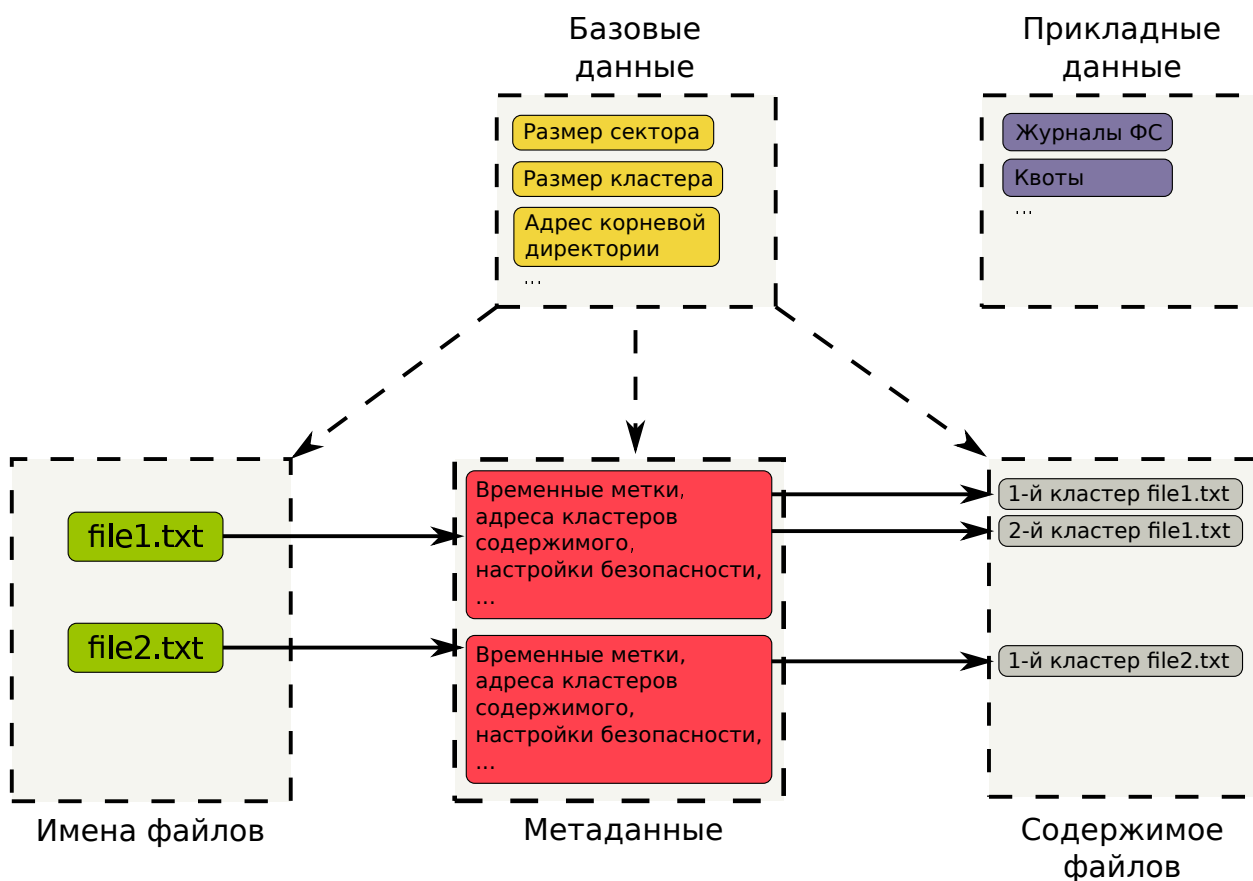


Рис. 26. Категории данных ФС и их взаимосвязи. Категория базовых данных оказывает свое влияние на другие категории данных, что выражается в том, что данные из базовых данных используются постоянно при работе с файлами. Прикладные данные остаются в стороне, так как они не задействованы напрямую в процессах доступа к файлам и зачастую являются опциональными (необязательными)

## 5.4. Безопасность операционной системы

### 5.4.1. Управление доступом

Для грамотной защиты информации ОС реализует некоторые формальные (математические) модели, задающие условия, при которых кто-либо может получить доступ к информации. Эти модели называются моделями управления доступом. В них есть своя устоявшаяся терминология, которой оперируют, когда речь заходит о защите информации. Введем основные понятия.

1. **Объекты доступа** — это данные, доступ к которым нужно разграничить. Чаще всего это файлы, но могут быть и другие объекты ОС: ключи реестра, объекты подключенных внешних носителей и других устройств и т. д.
2. **Субъекты доступа** — это пользователи ОС, от имени которых процессы и потоки осуществляют доступ к защищаемым объектам в ОС.
3. **Право доступа** — это разрешение, которое может быть предоставлено субъекту, на выполнение некоторого действия с объектом.

4. **Доступ**— это непосредственное выполнение действия субъектом доступа применительно к объекту доступа. Если действие не разрешено настроенными правами доступа, но тем не менее как-то было осуществлено, то такой доступ называют несанкционированным.

В современных ОС может применяться сразу несколько моделей управления доступом, а также дополнительные механизмы для разрешения или запрета определенных действий. В следующих пунктах познакомимся с самыми распространенными моделями.

#### 5.4.2. Дискреционное управление доступом

В этой модели каждый объект хранит **список управления доступом** — список пар (субъект, права доступа). Решение о доступе субъекта к объекту как раз и принимается на основе поиска пары с необходимым субъектом и правом доступа в списке управления доступом. Если пара найдена — ОС предоставит доступ, иначе не предоставит (смотри рисунок 27).

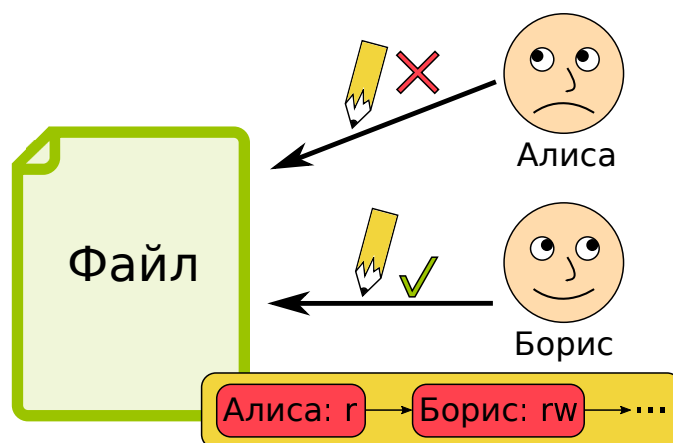


Рис. 27. Дискреционное управление доступом. Список управления доступом файла содержит пары (Алиса, r) и (Борис, rw), то есть у Алисы есть право чтения файла, а у Бориса чтения и записи. При таких правах Алисе запрещена запись в файл, а Борису разрешена. Чтение разрешено обоим, исполнение запрещено обоим

Обычно есть по крайней мере 3 основных права доступа: чтение (r), запись (w) и исполнение (x). Разберем действие этих прав на примере файла. Право чтения дает возможность читать содержимое файла, право записи дает возможность изменять содержимое файла, а право исполнения дает возможность запустить файл приложения, то есть инициировать запуск процесса этого приложения. Право доступа исполнения задается только тем файлам, которые ОС может выполнить как приложение. То есть тем, для которых ОС может создать процесс, который выполнит записанные в таком файле команды на процессоре.

#### 5.4.3. Ролевое разграничение доступа

Эту модель можно назвать логическим продолжением дискреционной модели. В ролевой модели можно создавать роли и назначать им права доступа на объекты, а

субъектов делать участниками ролей. То есть теперь решение о предоставлении доступа может быть принято не только тогда, когда в списке управления доступом объекта нашлась пара с нужным субъектом и нужным правом доступа, но и когда в списке нашлась пара с ролью, в которую входит субъект, и нужным правом доступа (смотри рисунок 28).

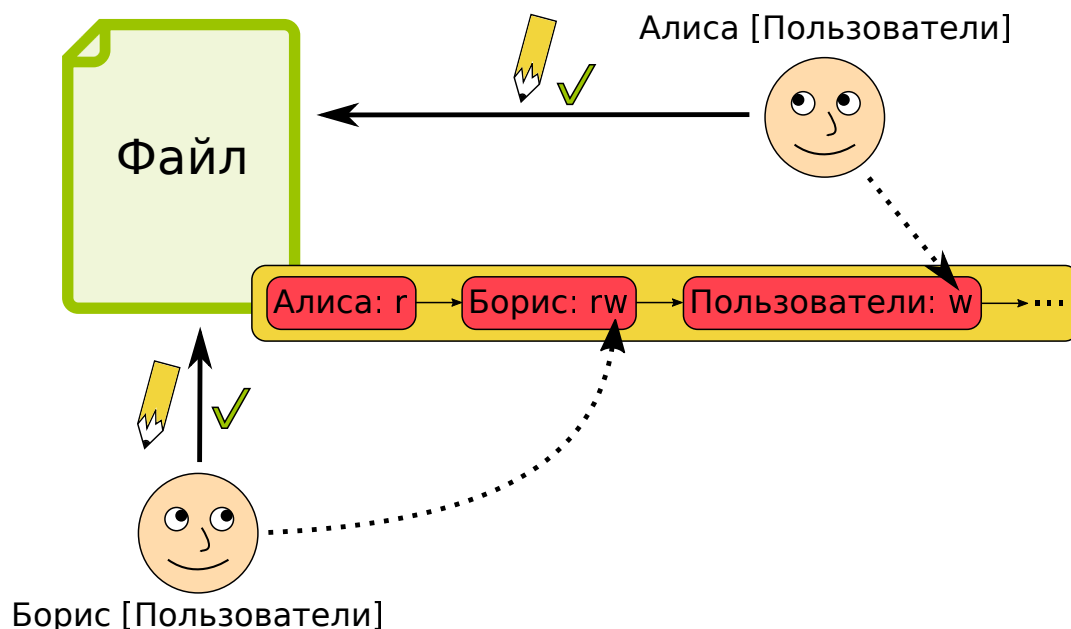


Рис. 28. Ролевое управление доступом. В сравнении с рисунком 27 Алиса может осуществить запись в файл, так как она входит в группу «Пользователи», и для этой группы разрешена запись в файл

Ролевая модель имеет очевидные преимущества по сравнению с дискреционной, так как позволяет разграничить доступ на файлах для группы пользователей с одинаковыми требованиями по доступу. Например, для разрешения запуска приложения, скажем, 100 пользователям ОС в дискреционной модели нужно в список управления доступом приложения добавить 100 записей для каждого пользователя с правом x. В ролевой же модели нужно всех пользователей добавить в группу (роль) «Пользователи» и добавить одну запись в список управления доступом файла приложения — («Пользователи», x).

#### 5.4.4. Мандатное управление доступом

Здесь каждому объекту присваивается уровень секретности (уровень доступа), а каждому субъекту уровень допуска. Скажем, уровни «секретно» с номером 0, «совершенно секретно» с номером 1 и «особой важности» с номером 2 для объектов. И 0, 1, 2 уровни допуска для субъектов. Прав доступа как в дискреционной модели выше. Далее доступ разграничивается следующим образом (смотри рисунок 29):

1. Операция записи разрешена, если уровень допуска строго равен номеру уровня секретности.
2. Операции чтения и исполнения разрешены, если уровень допуска больше или равен номеру уровня секретности.

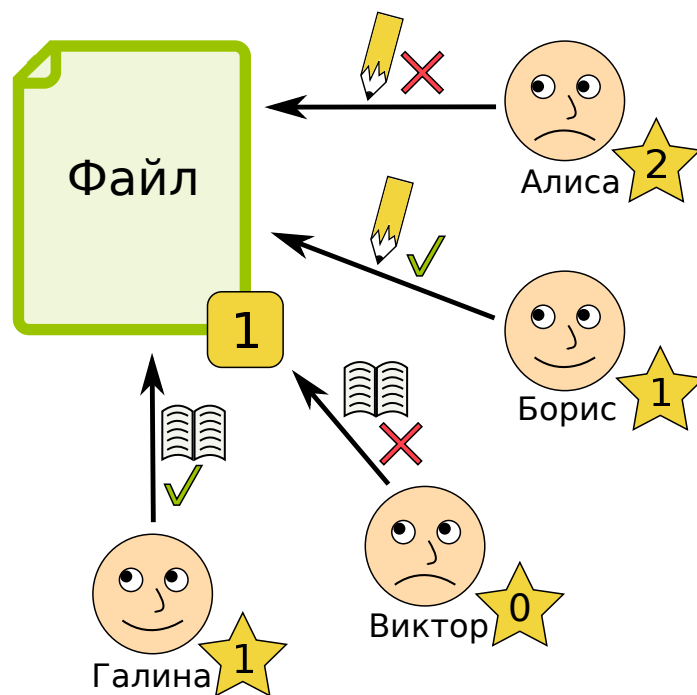


Рис. 29. Мандатное управление доступом. Уровень доступа файла равен 1. Уровни допуска субъектов указаны в звездах. Алисе запрещена запись, так как ее допуск выше, чем уровень доступа файла. Борису запись разрешена. Виктору запрещено чтение, так как его уровень допуска ниже, чем уровень секретности файла. Галина может читать файл

Обратим внимание на то, что мандатное управление доступом нацелено на обеспечение конфиденциальности данных. А именно исключаются чтение информации высокого уровня секретности субъектами с низким уровнем допуска, а также запись информации субъектами с высоким допуском в файлы с низким уровнем доступа: предотвращается дальнейшее считывание такого файла субъектом с низким допуском.

#### 5.4.5. Модель целостности Биба

Модель целостности Биба похожа на мандатное управление доступом, но во главу угла поставлена целостность, а не конфиденциальность. Пусть у каждого объекта и субъекта есть уровень целостности (по аналогии с уровнями в мандатном управлении доступом). Тогда доступ разграничивается следующим образом:

1. Операция записи разрешена, если уровень целостности субъекта больше или равен уровню целостности объекта.
2. Операции чтения и исполнения разрешены при любых уровнях целостности субъекта и объекта.

Если мандатное разграничение доступа обеспечивает конфиденциальность информации, то модель Биба нацелена на обеспечение целостности. Видно, что разграничивается только доступ на запись. Суть ограничения следующая: запретить субъектам с низким уровнем целостности «портить» важные документы или системные файлы, тем самым защищая целостность таких файлов.

#### 5.4.6. Привилегии

Кроме правил доступа субъектов к объектам, в ОС часто присутствует механизм привилегий.

**Привилегия** — это разрешение на выполнение какого-то специального действия. Часто привилегии разрешают такие действия, которые могут привести к обходу проверок подсистемы управления доступом. К примеру, в Windows есть привилегия SeBackupPrivilege, которая позволяет делать резервные копии файлов и директорий. Обладая этой привилегией, можно прочитать любой файл в системе в обход системы управления доступом (смотри рисунок 30).

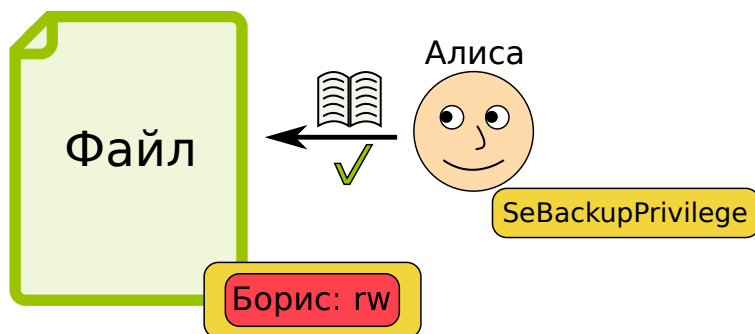


Рис. 30. Привилегии. Приведен пример в контексте ОС Windows, в котором у Алисы нет никаких прав на файл, но тем не менее она может прочитать содержимое файла, так как у нее есть привилегия SeBackupPrivilege

#### 5.4.7. Идентификация

Для реализации управления доступом в ОС субъекты должны быть пронумерованы, то есть им должны быть присвоены идентификаторы. Ранее было сказано, что субъектами в ОС являются пользователи. Пользователь в системе не обязательно создается для работы человека в ОС. Бывают пользователи, которые создаются специально для выполнения отдельных приложений. Бывают системные пользователи, от имени которых в ОС выполняются определенные процессы.

Системные пользователи получают свои идентификаторы при установке системы, пользователи приложений — при установке этих приложений, пользователи, под которыми в системе работают люди, создаются на этапе установки или регистрируются в системе в дальнейшем.

Идентификацией называется процесс, в результате выполнения которого для субъекта доступа выявляется его идентификатор (смотри рисунок 31).

#### 5.4.8. Аутентификация

**Аутентификация** — процесс доказательства того, что лицо, представляющееся системе определенным именем, действительно то, за кого себя выдает.

До сих пор в ОС самым распространенным способом аутентификации остается парольная. Если было введено правильное имя и пароль, то система считает, что лицо именно то, за кого себя выдает.

Разберемся в процессе парольной аутентификации (смотри рисунок 32):

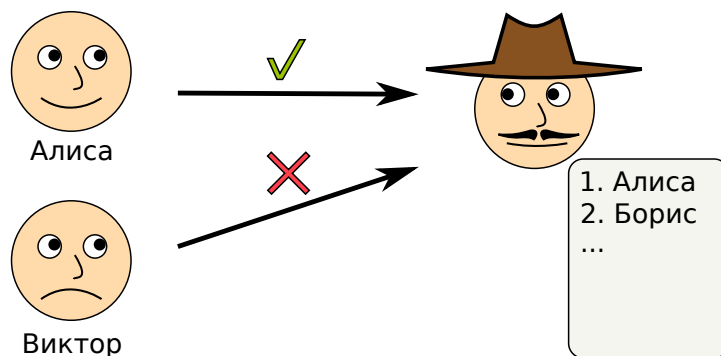


Рис. 31. Идентификация. Алиса представляется Алисой, и система определяет ее номер — 1. Виктора нет в списке, значит, у него нет номера и он не может пройти процесс идентификации

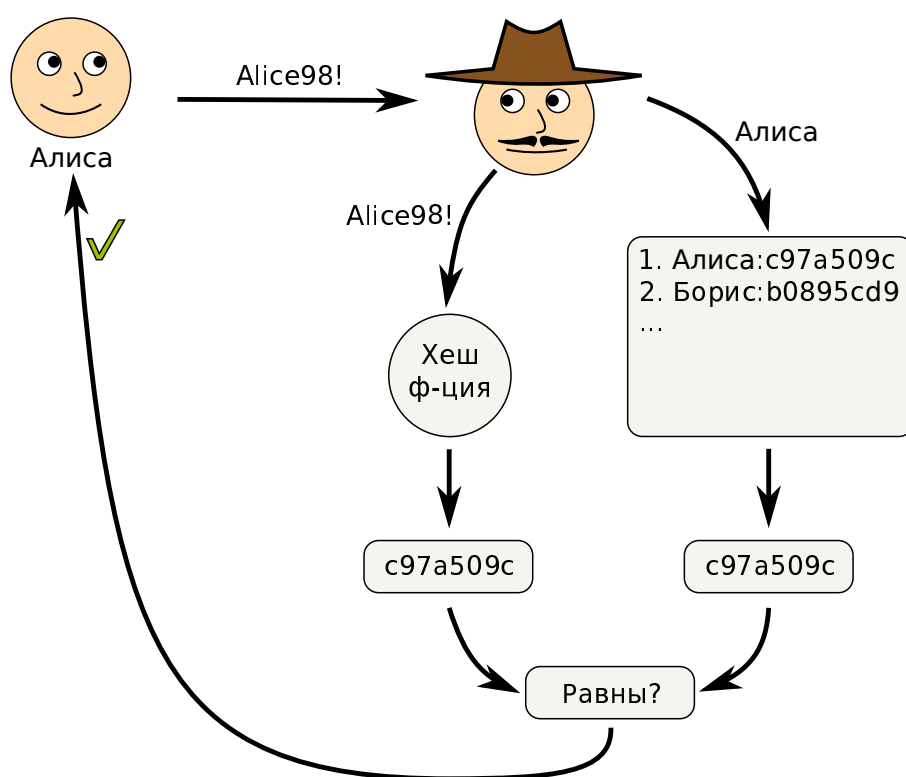


Рис. 32. Процесс парольной аутентификации

1. Пользователь вводит логин и пароль в аутентифицирующее приложение.
2. Приложение считает хеш-функцию от пароля.
3. Приложение считывает с диска эталонное значение хеш-функции пароля.
4. Если значения хеш-функций совпали, то ОС разрешает вход пользователю, иначе нет.

Биометрическая аутентификация не имеет концептуальных отличий от парольной. «Паролем» в данном случае являются оцифрованные биометрические данные:



отпечаток пальца, лицо, отпечаток ладони, ДНК, радужная оболочка глаза и т. д. При этом на диске также хранится эталонное значение, по которому нельзя воссоздать изначальные данные о человеке и на основе которого принимается решение о разрешении входа. Различия от парольной аутентификации здесь в основном в технологических тонкостях сбора и обработки аутентификационной информации. Очевидное преимущество биометрической аутентификации в том, что обмануть биометрические сканеры, подделав, скажем, отпечаток пальца, гораздо сложнее, чем напечатать украденный пароль.

Аутентификация на основе внешнего носителя ключа (**токена**) значительно отличается от парольной. На таком носителе содержится закрытый ключ асимметричного алгоритма шифрования. Все, что нужно, чтобы система могла аутентифицировать пользователя по такому ключу, — это наличие соответствующего криптопровайдера, умеющего работать с необходимым асимметричным алгоритмом, и наличие в системе открытого ключа, связанного с пользователем. Затем процесс аутентификации может идти следующим образом (смотри рисунок 33):

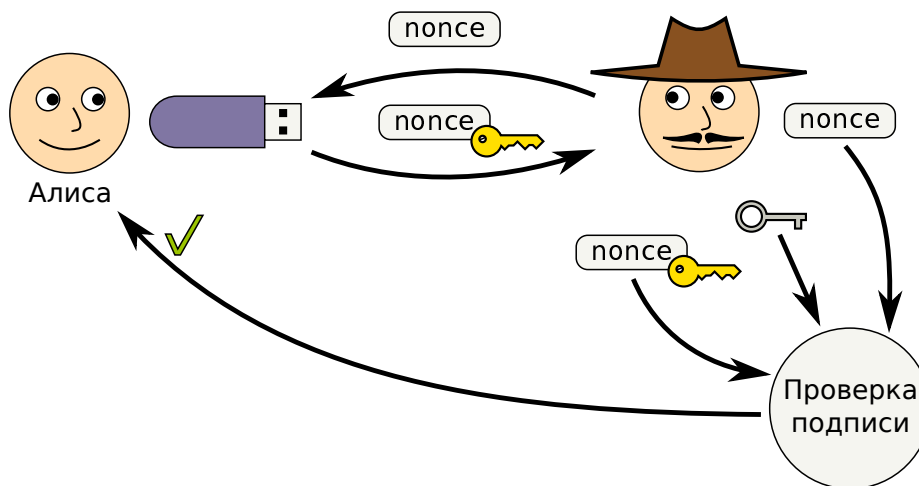


Рис. 33. Процесс аутентификации на основе внешнего носителя ключа. nonce — случайная строка

1. ОС передает во внешний носитель случайную строку с просьбой подписать ее закрытым ключом.
2. Внешний носитель создает цифровую подпись этой строки и возвращает ее в ОС.
3. ОС проверяет правильность подписи открытым ключом. Если подпись верна, то вход разрешен, иначе нет.

Безопасность такой системы аутентификации довольно высока, пока токен не украден, так как токены конструктивно сделаны так, чтобы считать закрытый ключ было невозможно. Для защиты от использования украденного токена используют защиту PIN-кодом.

#### 5.4.9. Авторизация

**Авторизация** — процесс проверки соответствия доступа заданным в системе правам доступа.

Авторизация в современной ОС — это сложный процесс в силу того, что в системе зачастую реализованы идеи из разных моделей управления доступом, а также есть некоторые механизмы, которые позволяют в некоторых ситуациях полностью игнорировать назначенные в системе права доступа. Тот порядок, в котором учитываются назначенные настройки безопасности на субъектах и объектах доступа при осуществлении доступа, и определяет процесс авторизации.

Процессов авторизации мы коснемся более подробно в разделах 6 и 7.

## 5.5. Вопросы и задания

**5.1.** Пусть в ОС реализовано дискреционное управление доступом со следующими правами: чтение (r), запись (w) и исполнение (x). Присутствует файл приложения «Калькулятор.exe» со следующим списком доступа: (Алиса: rwx), (Борис: rx). Выберите правильные утверждения:

1. Алиса может запустить приложение «Калькулятор.exe».
2. Борис не может запустить приложение «Калькулятор.exe».
3. Алиса не может изменить содержимое файла «Калькулятор.exe».
4. Борис может изменить содержимое файла «Калькулятор.exe».

**5.2.** Пусть в ОС реализовано групповое управление доступом со следующими правами: чтение (r), запись (w) и исполнение (x). Присутствует файл «Накладная.docx» со следующим списком доступа: (Бухгалтеры: rw), (Курьеры: r), (Алиса: rw). В системе заданы роли, в которые включены соответствующие пользователи: (Бухгалтеры: Борис, Галина), (Курьеры: Виктор). Выберите правильные утверждения:

1. Борис не может изменить содержимое файла «Накладная.docx».
2. Галина может читать содержимое файла «Накладная.docx».
3. Виктор может изменить содержимое файла «Накладная.docx».
4. Виктор может читать содержимое файла «Накладная.docx».
5. Алиса может изменить содержимое файла «Накладная.docx».

**5.3.** Пусть в ОС реализовано мандатное управление доступом. Присутствует файл «log.txt» с уровнем секретности 1. Присутствуют пользователи Алиса с уровнем допуска 1, Борис с уровнем допуска 2 и Виктор с уровнем допуска 0. Выберите правильные утверждения:

1. Виктор может изменить содержимое файла «log.txt».
2. Виктор может читать содержимое файла «log.txt».
3. Алиса может изменить содержимое файла «log.txt».
4. Алиса может читать содержимое файла «log.txt».
5. Борис может изменить содержимое файла «log.txt».

6. Борис может читать содержимое файла «log.txt».

**5.4.** Пусть в ОС реализована модель целостности Биба. Присутствует файл «log.txt» с уровнем целостности 1. Присутствуют пользователи Алиса с уровнем целостности 1, Борис с уровнем целостности 2 и Виктор с уровнем целостности 0. Выберите правильные утверждения:

1. Виктор может изменить содержимое файла «log.txt».
2. Алиса может изменить содержимое файла «log.txt».
3. Борис может изменить содержимое файла «log.txt».
4. Все трое могут читать содержимое файла «log.txt».

**5.5.** Выберите правильные утверждения об аутентификации в современных ОС:

1. Пароли пользователя хранятся на диске, на котором установлена система, в первоначальном виде.
2. Эталонные значения, необходимые для прохождения биометрической аутентификации, хранятся в системе в недостаточном для восстановления изначальных биометрических данных объеме.
3. Токен физически изготовлен таким образом, что считывание с него закрытого ключа является невозможной или дорогостоящей операцией.
4. Для аутентификации с помощью токена в системе должен присутствовать открытый ключ пользователя, соответствующий закрытому ключу на его токене.

**5.6.** Какие параметры входят в метаданные файла?

**5.7.** Выберите верные утверждения об управлении памятью в современных ОС:

1. Современные ОС используют виртуальную память.
2. Современные ОС не защищают память одних процессов от чтения другими процессами.
3. Современные ОС разделяют общую память между процессами, часто в такой памяти находятся библиотеки.
4. Современные ОС никогда не выгружают части оперативной памяти на диск во время работы.
5. В современных ОС память разбита на маленькие фрагменты, называемые страницами.

**5.8.** Выберите верные утверждения о планировщике:

1. Планировщик выделяет процессорное время короткими интервалами, называемыми квантами.

2. В случае исполнения процессом инструкции, для завершения которой требуется длительное ожидание, планировщик переводит процесс в состояние «заблокирован» и не будет выделять ему процессорное время, пока состояние не сменится на «готов».
3. Для работы планировщика процессы должны сами передавать на него управление, так как компьютеры не предоставляют ОС механизма для периодического прерывания выполнения пользовательского процесса.
4. В планировании по приоритетам все процессы с разными приоритетами получают примерно одинаковое количество времени.

**5.9.** Выберите верное утверждение (выберите один вариант):

1. ОС реализована аппаратно в процессоре.
2. ОС реализована аппаратно в материнской плате.
3. ОС — программное обеспечение, которое предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных абстракций, но не управляет этим аппаратным обеспечением.
4. ОС — программное обеспечение, которое предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных абстракций и управляет этим аппаратным обеспечением.

**5.10.** Выберите верное утверждение (выберите один вариант):

1. В ОС компьютера с одноядерным процессором в каждый момент времени может работать только один процесс.
2. В ОС компьютера с одноядерным процессором у процессов всегда присутствует только один поток.
3. В ОС компьютера с многоядерным процессором в конкретный момент времени могут выполняться несколько потоков одного процесса.
4. В ОС компьютера с многоядерным процессором конкретный процесс может использовать только одно ядро процессора.

## 6. Безопасность ОС Windows

Модель безопасности Windows — сложная многомодульная система, в которой встречаются ролевой доступ, модель целостности Биба, мандатный доступ, привилегии, в которой доступы к разным объектам осуществляются по-разному, разные субъекты ведут себя по-разному и т. д. В этом разделе будут затронуты только основы безопасности Windows, однако это та база, на которой работает вся безопасность Windows.

### 6.1. Субъекты доступа

В Windows субъект доступа характеризуется **токеном доступа**. По факту это означает, что процесс, поток которого осуществляет доступ к объекту, обладает этим токеном, содержащим всю необходимую для проверки возможности доступа информацию. Токен доступа процесса называют **первичным**. Поток процесса может иметь свой токен доступа, называемый **impersonation token**, что можно перевести на русский как **токен перевоплощения**. Этот токен используется системой, когда поток должен выполнить какое-то действие от имени пользователя, который отличен от указанного в первичном токене.

Опишем содержимое токена доступа.

#### 6.1.1. Токен доступа

Отметим, что в токене множество полей относится к некоторому пользователю, это пользователь, от имени которого был запущен процесс. Токен доступа состоит из множества полей, укажем основные, используемые для управления доступом:

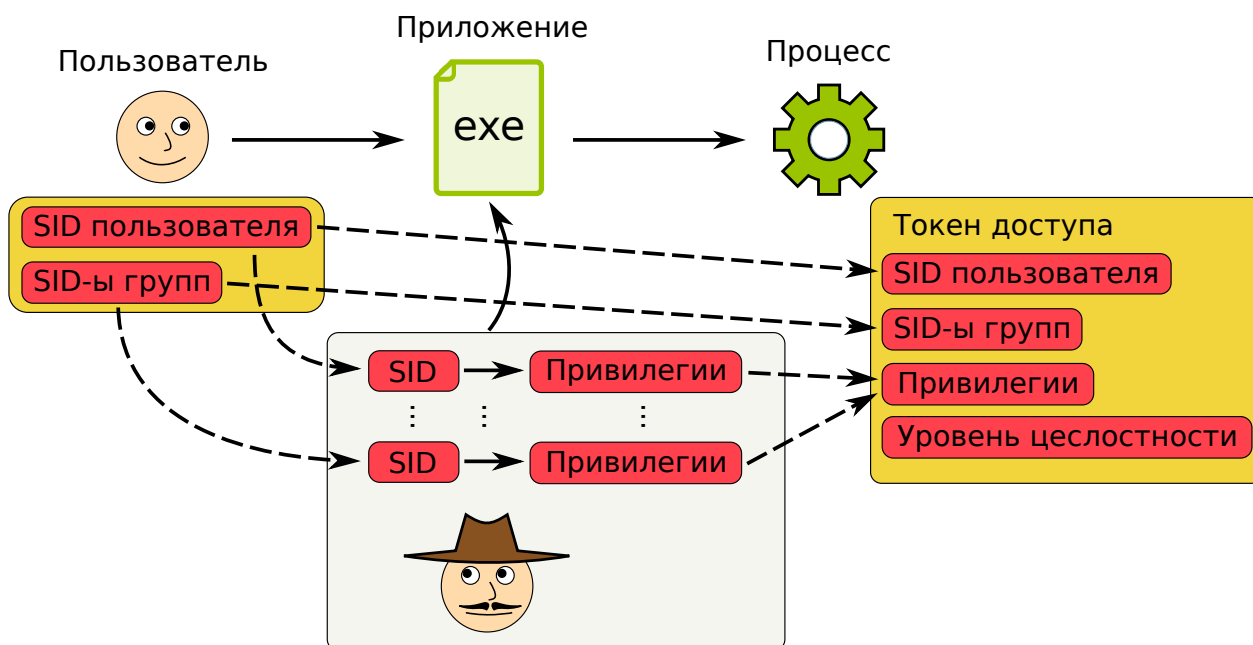


Рис. 34. Схема формирования токена доступа

- Идентификатор пользователя.

- **Идентификаторы групп**, в которые входит пользователь.
- **Уровень целостности**, на котором запущен процесс.
- **Список привилегий**, выданных пользователю или группам, в которые входит пользователь.

Схему формирования токена доступа при запуске пользователем приложения можно увидеть на рисунке 34.

### 6.1.2. Идентификаторы

Для идентификации пользователей и групп в Windows используются **идентификаторы безопасности (security identifier, SID)**. Идентификаторы состоят из 5 частей:

1. **Версия**. Сейчас это первая версия, то есть эта часть равна «1».
2. **Область применения**, для Windows-систем зарезервировано число «5».
3. **Первая подобласть применения**. Значение «21» , например, применяется при идентификации пользователей и групп, являющихся уникальными для конкретных систем или доменов Windows; «32» — для локальных пользователей, например, локальный (не доменный) администратор системы или локальная группа администраторов.  
Некоторые значения в этой области являются последними в SID и принадлежат некоторым системным пользователям: «S-1-5-18» — «**локальная система**» — специальный высокопривилегированный пользователь, используемый ОС Windows; «S-1-5-19» — «**локальный сервис**» — специальный пользователь, используемый сервисами ОС Windows; «S-1-5-20» — «**сетевой сервис**» — специальный пользователь ОС Windows для сервисов, которым необходимо иметь доступ к учетным данным пользователя для работы от его лица в сети и т. д.
4. **Вторая подобласть применения** — массив чисел для однозначной идентификации компьютера или домена.
5. **Относительный идентификатор** — уникальный идентификатор субъекта внутри домена.

Части идентификатора записываются через дефис. Числа из массива четвертой части также записываются через дефис. В начале SID-а пишется «S-». Например, «S-1-5-21-3610261748-2700554493-1936302053-1001» — SID первой версии, относящийся к Windows, к конкретной машине или домену, уникальный номер которого равен «3610261748-2700554493-1936302053», к пользователю или группе «1001».

### 6.1.3. Уровни целостности

ОС Windows оперирует шестью первичными уровнями целостности (список от низкого уровня доступа к высокому):

1. **Недоверенный** — используется процессами, запущенными анонимными пользователями.

2. **Низкий** — используется для запуска процессов в песочницах<sup>11</sup> и в современных браузерах для защиты от записи в важные системные файлы.
3. **Средний** — используется обычными приложениями.
4. **Высокий** — используется приложениями, запущенными от имени администратора.
5. **Системный** — используется системными процессами и сервисами.
6. **Защищенный** — в целом не используется, но может быть установлен в режиме ядра.

Относительно уровня целостности процессов действуют следующие правила:

1. Обычно процесс наследует уровень целостности от запустившего его процесса.
2. Если исполняемый файл программы обладает заданным уровнем целостности и эта программа запускается процессом со средним или высоким уровнем, то новому процессу будет присвоен наименьший уровень из двух перечисленных.
3. Процесс может запустить дочерний процесс с уровнем целостности ниже своего.

#### 6.1.4. Привилегии

Пользователю или группе в Windows могут быть выданы привилегии. Всего в Windows присутствует 36 привилегий. Перечислим только те из них, обладание которыми равносильно полному контролю над компьютером. Выдача таких привилегий обычным пользователям недопустима, так как ведет к полной компрометации системы. Список наиболее опасных привилегий:

- **Привилегия отладки (SeDebugPrivilege)** — позволяет подключаться к любым процессам в системе другим процессом — **отладчиком**. Отладчик может полностью контролировать исполнение другого процесса, читать и изменять его память. Зловредный процесс с такой привилегией может открыть для отладки высокопривилегированный процесс, записать в его память зловредный код и передать на него управление.
- **Привилегия взятия владения (SeTakeOwnershipPrivilege)** — позволяет взять во владение объект. Далее мы узнаем, что владелец объекта может менять права на объекте. Соответственно, зловредный процесс с такой привилегией может записать свой код в любой файл в системе (например, файл ядра ОС), взяв его во владение и предоставив себе доступ на запись.
- **Привилегия восстановления (SeRestorePrivilege)** — позволяет заменять любой файл в NTFS. Используется для восстановления файлов. Зловредный процесс с такой привилегией может восстановить свою версию ядра ОС Windows.
- **Привилегия загрузки драйверов (SeLoadDriverPrivilege)** — позволяет загружать драйвера в ОС. Зловредный процесс может загрузить драйвер со своим кодом в систему и выполнять зловредный код в режиме ядра.

---

<sup>11</sup>Механизм, встречающийся во многих ОС, позволяющий исполнять недоверенные приложения, значительно ограничив их права в системе.

- **Привилегия создания токена доступа (SeCreateTokenPrivilege)** — позволяет создавать токен доступа. Такая привилегия не ведет к легкой компрометации системы, так как создать токен мало, нужно создать процесс или поток с повышенным уровнем доступа. Однако существуют техники, которые позволяют полностью скомпрометировать систему, обладая такой привилегией.
- **Привилегия действия от имени ОС (SeTcbPrivilege)** — при некоторых действиях в системе позволяет выступать от ее имени. Не углубляясь в подробности, отметим, что эта привилегия так же опасна, как предыдущие.

Есть и другие опасные привилегии. Например, **привилегия создания резервных копий (SeBackupPrivilege)** позволяет читать любой файл в системе, в том числе ключи реестра, в которых хранится хеш пароля пользователя. Так как в Windows до сих пор довольно слабая система хеширования, зная хеш простого пароля, можно довольно быстро подобрать пароль. Привилегии **перевоплощения (SeImpersonatePrivilege)** и **присвоения первичного токена (SeAssignPrimaryTokenPrivilege)** совместно могут открывать возможности для повышения уровня доступа в системе.

При этом есть и такие, которые не несут какую-то серьезную угрозу безопасности, например, **привилегия изменения системного времени (SeSystemtimePrivilege)**.

## 6.2. Объекты доступа

У каждого объекта доступа в Windows есть **дескриптор безопасности**. Дескриптор безопасности объекта вкупе с токеном доступа субъекта позволяют системе сделать вывод о том, разрешен ли конкретный доступ субъекта к объекту.

### 6.2.1. Дескриптор безопасности

Перечислим основные поля дескриптора безопасности (смотри рисунок 35):

- **SID владельца.**
- **Дискреционный список управления доступом (ДСУД).**
- **Системный список управления доступом (ССУД).** Этот список так же, как ДСУД, содержит записи, в которых указан субъект доступа и права доступа. Эти записи наследуются по тем же правилам. Различие в том, что этот список служит не для разграничения доступа, а для аудита. Запись указывает тип события, при каком событии сделать запись в журнал аудита: при успешном доступе, при отказе в доступе или при обоих событиях.

Также в ССУД указывается уровень целостности объекта.

### 6.2.2. Дискреционные списки управления доступом

В целом это обычный список управления доступом ролевой модели управления доступом, в котором для каждого пользователя или группы указаны разрешенные доступы. При этом есть существенные отличия от списка, который используется в классической модели:



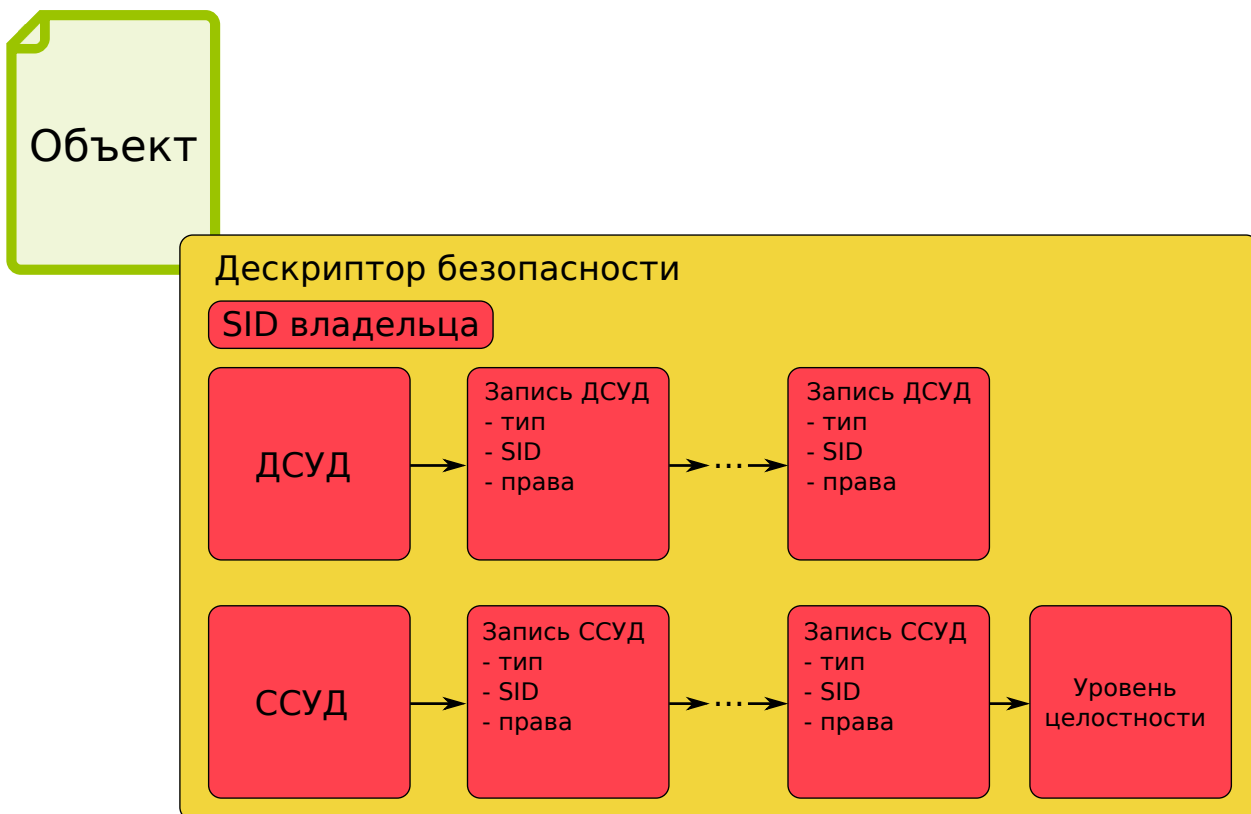


Рис. 35. Дескриптор безопасности

- Кроме базовых прав чтения, записи и исполнения, присутствуют и другие права. Всего их 23, но большинство — это комбинация базовых. Приведем некоторые из базовых прав:
  - **Чтение системных атрибутов** — право чтения системных атрибутов файла, таких как время создания файла, размер файла и пр. Не включает право чтения атрибутов безопасности и данных.
  - **Чтение атрибутов безопасности** — право чтения атрибутов безопасности (ДСУД и ССУД). Не включает право чтения системных атрибутов и данных.
  - **Чтение данных (просмотр содержимого директории)** — право чтения содержимого файла (для файла) или имен внутрилежащих файлов (для директории). Не включает право чтения системных атрибутов и атрибутов безопасности.
  - **Запись атрибутов** — право изменения системных атрибутов файла. Не включает право изменения атрибутов безопасности и данных.
  - **Изменение атрибутов безопасности** — право изменения атрибутов безопасности файла. Не включает право изменения системных атрибутов и данных.
  - **Запись данных (создание файлов в директории)** — право изменения содержимого файла (для файла) или создания поддиректорий и файлов (для директории). Не включает право изменения системных атрибутов и атрибутов

безопасности. Не дает права удаления файла или файлов и поддиректорий в директории.

- **Добавление данных (создание поддиректорий** в директории) — право дозаписи в файл (для файла) или создания поддиректорий (для директории).
- **Выполнение файлов (переход** в директорию) — право запуска файла программы или доступа к файлу внутри директории.
- **Удаление поддиректорий и файлов** — право удаления поддиректорий и файлов в директории.
- **Удаление** — право удаления файла или директории. У субъекта может быть право удаления файла или директории без этого права, если у него есть право «удаление поддиректорий и файлов» на родительскую директорию.

Например, право «чтение» объединяет права «чтение системных атрибутов», «чтение атрибутов безопасности», «чтение данных» и «чтение расширенных атрибутов» (последнее право не упоминалось, мы его не будем рассматривать).

- Запись списка доступов обладает типом. Всего их девять, но мы рассмотрим лишь два. Это разрешающий или запрещающий тип. Разрешающий тип записи — это стандартный тип, который встречался нам в описании дискреционной модели доступа: права, указанные в такой записи, разрешают соответствующие доступы субъекту. Запрещающая запись имеет противоположный смысл. То есть в Windows можно запретить определенный вид доступа с помощью создания запрещающей записи для субъекта с соответствующим правом.
- Некоторые объекты поддерживают структуру вложенности, например, NTFS-файлы и ключи реестра. В таких структурах есть контейнеры (директории, пространства имен реестра) и непосредственно объекты (файлы, ключи реестра). Windows поддерживает наследование правил доступа и аудита от родительских контейнеров дочерними контейнерами и файлами.

Для распространения прав каждая запись ДСУД содержит флаги распространения:

- **Наследована** — означает, что эта запись унаследована от родительских контейнеров, и она будет учтена при разграничении доступа.
- **Только для наследования** — означает, что эта запись используется только для передачи дочерним контейнерам и объектам. Применяется на контейнерах, не будет учитываться при разграничении доступа к этим контейнерам.
- **Наследовать в контейнерах** — эта запись будет повторена в дочерних контейнерах с флагами «наследована» и «наследовать в контейнерах». Цепочку наследования по контейнерам может прервать явное применение флага «не наследовать» на очередном контейнере.
- **Наследовать в объектах** — эта запись будет повторена в дочерних контейнерах с флагами «только для наследования» и «наследовать в объектах», и с флагом «наследована» в дочерних объектах.
- **Не наследовать** — убирает флаги «наследовать в контейнерах» и «наследовать в объектах» с записи.

Флаги могут комбинироваться, например, комбинация «наследовать в контейнерах» и «наследовать в объектах» предписывает ОС учитывать права данной записи при разграничении доступа к дочерним контейнерам и объектам.

### 6.2.3. Уровни целостности

Уровень целостности объекта задает **мандатная метка**, в которой хранится одно из значений из списка уровней целостности, приведенного в подсекции 6.1.3.

Также для каждого объекта задана **мандатная политика**, которых в Windows присутствует три:

- **No-Write-Up (Не-Записывать-Вверх)**: неявно используется для всех объектов доступа. Запрещает запись в объекты с уровнем целостности большим, чем у процесса.

По сути это реализация модели целостности Биба на уровне системы относительно всех объектов доступа.

- **No-Read-Up (Не-Читать-Вверх)**: используется только для объектов процессов (в Windows процесс — также защищаемый объект доступа). Запрещает читать из объектов с большим уровнем целостности, чем у читающего процесса. Применение этой политики к процессам предотвращает утечку информации из памяти процесса, осуществляемую со стороны другого процесса.

Это фактически реализация мандатного управления доступом, но только для процессов. Для других объектов, например, NTFS-файлов эта политика не работает.

- **No-Execute-Up (Не-Исполнять-Вверх)**: назначена исполняемым файлам, реализующим COM классы (COM — Component Object Model — программные компоненты Windows для межпроцессорного взаимодействия). Запрещает исполнять код объекта с определенным уровнем целостности процессу с более низким уровнем целостности. Применение данной политики призвано запретить процессам с низким уровнем целостности вызывать предоставляемые через COM-интерфейсы функции процессов с более высоким уровнем целостности.

### 6.3. Права владельца

В системе присутствует специальный SID «S-1-3-4» для «**прав владельца**». Права владельца на конкретные объекты могут задаваться администратором системы. По умолчанию владельцу разрешено читать и изменять ДСУД. И даже если никаких других прав владельцу не дано, он всегда может задать права для полного доступа к файлу, которым он владеет, в ДСУД, и получить необходимый доступ. Однако с помощью создания записи с SID «S-1-3-4» в качестве субъекта доступа, администратор может назначить произвольные права для владельца. В том числе запретить владельцу читать и изменять ДСУД.

### 6.4. Алгоритм определения правомерности доступа

Для определения правомерности доступа используются следующие шаги:

1. Определяются уровни целостности объекта и субъекта, а также мандатная политика объекта. Если доступ противоречит мандатной политике, то доступ запрещается.
2. Если у объекта нет ДСУД, то доступ разрешен.
3. Если на объекте заданы права владельца, то принять их за текущий доступ. Иначе принять за текущий доступ права на чтение и запись ДСУД.
4. Для каждой записи в ДСУД выполнить:
  - а) Если запись разрешающая и SID владельца или SID одной из групп в токене доступа равен SID-у в записи, то добавить права из записи к правам в текущем доступе. Если на этом шаге все необходимые для доступа права есть в текущем доступе, то разрешить доступ.
  - б) Если запись запрещающая и SID владельца или SID одной из групп в токене доступа равен SID-у в записи, и хотя бы одно из требуемых прав доступа содержится в записи, то запретить доступ.
5. Если дошли до этого шага и в текущем доступе не оказалось всех необходимых для доступа прав, то доступ запрещен.

## 6.5. Аудит

Аудит в Window можно настроить как на отдельные файлы, задавая списки ССУД, так и глобально. В частности, можно настроить глобальный аудит доступа к файлам или ключам реестра для конкретного пользователя или группы: настраивать ССУД для каждого файла отдельно в таком случае не нужно. При этом можно указать основные виды доступов, подлежащие аудиту: чтение, запись и выполнение. Для настройки глобального аудита используется утилита **auditpol**.

То, какие события будут помещены в журнал аудита, также контролируется настройками в политике безопасности, в ней можно настраивать аудит на одну из девяти категорий действий в системе:

- **Аудит входа в систему:** аудит входов в систему и выходов из нее. Эти события связаны с созданием или удалением сеанса работы пользователя соответственно.
- **Аудит доступа к объектам:** аудит доступов к объектам, не относящимся к объектам домена Windows.
- **Аудит доступа к службе каталогов:** аудит доступов к объектам домена Windows.
- **Аудит изменений политики:** аудит изменений, вносимых в политику аудита.
- **Аудит использования привилегий:** аудит доступов, полученных с помощью привилегий.
- **Аудит отслеживания процессов:** аудит таких действий, как создание и завершение процессов.

- **Аудит системных событий:** отслеживание важных системных событий, например, сбой системы аудита, превышение журналом безопасности отведенного размера, загрузка нового модуля аутентификации и т. п.
- **Аудит событий входа в учетную запись:** отслеживание событий проверки учетных данных пользователя. Например, при входе с заблокированного экрана.
- **Аудит управления учетными записями:** аудит событий создания, изменения, удаления пользователей и групп.

## 6.6. Аутентификация

Если речь идет о стандартной парольной аутентификации, то Windows, как и другие системы, хранит хеш-значение пароля пользователя на диске. В системе он находится в специальном защищенном ключе реестра. Отметим, что получение хешей паролей Windows критично с точки зрения безопасности, так как в основе используется слабая хеш функция MD-5.

Отдельно отметим один механизм безопасности, связанный с аутентификацией, появившийся в Windows Vista — **UAC (user account control)**. Этот механизм призван защитить систему от атак повышения привилегий, запущенных от имени пользователя, входящего в одну из групп администраторов, или самого администратора (далее называем такого пользователя просто администратором). Достигается защита путем модифицирования токена доступа процессов, запускаемых администратором без применения функции «Запуск от имени администратора», следующим образом:

- Уровень целостности устанавливается средним.
- В токене доступа SID административных групп помечаются как **только запрещающие**. На текущий доступ при определении доступа в алгоритме секции 6.4 будут влиять только запрещающие записи ДСУД с такими SID. То есть прав администратора, предоставляемых на основе дискреционного доступа, запущенный процесс не получит.
- Оставляются только привилегии SeChangeNotifyPrivilege, SeShutdownPrivilege, SeUndockPrivilege, SeIncreaseWorkingSetPrivilege и SeTimeZonePrivilege. Все остальные привилегии не попадают в токен доступа.

Когда приложение запускается от имени администратора, система требует итеративного вмешательства пользователя во всплывающем окне, отображаемом на отдельном рабочем столе. При этом, если пользователь не является администратором, а только входит в административную группу, то у него будет запрошен пароль администратора. При разрешении запуска приложения во всплывающем окне, приложению будет выдан неусеченный токен доступа и оно получит административные права в системе.

## 6.7. Вопросы и задания

- 6.1. На основе каких данных субъекта ОС Windows принимает решение о доступе?
- 6.2. На основе каких данных объекта ОС Windows принимает решение о доступе?

**6.3.** Какие примитивные права объединяет в себе право чтения ОС Windows?

**6.4.** Выберите правильные утверждения о мандатной политике «Не-Записывать-Вверх» ОС Windows:

1. Обеспечивает свойство целостности данных.
2. Обеспечивает свойство конфиденциальности данных.
3. Используется в системе только для объектов сетевых сокетов.
4. Неявно используется для всех NTFS-файлов.
5. Разрешает доступ на запись только субъектам с уровнем целостности, равным или большим по отношению к уровню целостности объекта доступа.

**6.5.** Какие из перечисленных прав ОС Windows предоставляет по умолчанию владельцу файла?

1. Читать ССУД.
2. Читать ДСУД.
3. Читать содержимое файла.
4. Изменять ДСУД.
5. Изменять ССУД.
6. Изменять содержимое файла.

**6.6.** Выберите правильные утверждения относительно алгоритма определения правомерности доступа ОС Windows:

1. Первым действием является проверка соответствия доступа мандатной политике.
2. Проверка соответствия доступа мандатной политике осуществляется после анализа записей ДСУД.
3. Если при последовательном анализе записей ДСУД оказывается, что одно из запрашиваемых прав запрещается в текущей записи, то доступ запрещается.
4. Если при последовательном анализе записей ДСУД разрешающие права текущей записи в сумме с разрешающими правами предыдущих записей перекрыли все запрашиваемые права, то доступ разрешается.
5. Если в списках ДСУД не было запрещающих запрашиваемые права записей и в то же время все разрешающие записи не перекрыли запрашиваемые права, то доступ запрещается.

**6.7.** Какая привилегия ОС Windows позволяет читать любой файл вне зависимости от заданных прав?

**6.8.** Выберите сущности, не входящие в токен доступа в ОС Windows:

1. SID пользователя.
2. ДСУД всех объектов системы.
3. SID-ы групп.
4. ССУД всех объектов системы.
5. Привилегии.

**6.9.** Выберите сущности, входящие в дескриптор безопасности объекта в ОС Windows:

1. SID владельца объекта.
2. Дискреционный список управления доступом.
3. Системный список управления доступом.
4. Список токенов доступа процессов, осуществляющих доступ к объекту.
5. Уровень целостности.

**6.10.** Какие из пунктов правильно описывают фильтрованный токен доступа администратора в ОС Windows?

1. Уровень целостности устанавливается средним.
2. Уровень целостности устанавливается высоким.
3. Список привилегий, которые могут попасть в фильтрованный токен, сильно ограничен.
4. При определении правомерности доступа среди записей ДСУД с SID административных групп будут учтены только запрещающие.
5. Списки привилегий одинаковы в обычном и фильтрованном токене доступа администратора.

## 7. Безопасность ОС Linux

### 7.1. Субъекты доступа

В отличие от ОС Windows, в ОС Linux на уровне ядра не разделяются понятия процесса и потока. Процесс в Linux — это главный (запускаемый при старте процесса) поток исполняемого приложения. Поэтому можно сказать, что в Linux пользователи взаимодействуют с объектами доступа только посредством потоков.

Для задач авторизации у каждого потока Linux присутствует структура **cred** (от англ. **credential** — «учетные данные»), основными полями которой являются следующие:

- **User ID, UID** — идентификатор пользователя, запустившего поток.
- **Effective UID, EUID** — эффективный (текущий) UID. В отличие от UID может меняться по определенным правилам, чтобы позволить потоку выполнить действия с правами другого пользователя.
- **Group ID, GID** — идентификатор группы по умолчанию пользователя, запустившего поток.
- **Effective GID, EGID** — эффективный (текущий) GID. Аналогично EUID может меняться, чтобы позволить потоку выполнить действия с правами другой группы.
- **Дополнительные группы пользователя**, запустившего поток.
- **Привилегии** (в ОС Linux называются «**capabilities**», «**возможности**») — привилегии потока (смотри подраздел 7.1.4).

Схему формирования учетных данных при запуске пользователем приложения можно увидеть на рисунке 36. О том, как именно атрибуты файла влияют на учетные данные процесса, рассказано в подразделах 7.1.3 и 7.1.4.

#### 7.1.1. Пользователи

Каждый пользователь в ОС Linux ассоциирован с уникальным идентификатором — **user identifier, UID**. UID в Linux является целым числом и чаще всего для современных систем является 32-битным. Информация о всех пользователях в системе записана в файле `/etc/passwd`, из которого можно узнать в том числе UID конкретного пользователя.

Стоит выделить пользователя с UID равным нулю. Пользователь с таким UID является суперпользователем (суперадминистратором) системы и может выполнять почти любое действие в ней. Чаще всего именем этого пользователя в системе является «**root**», но имя можно сменить. Ключевой характеристикой является именно значение UID.

Отметим, что исторически пользователю также соответствует одна **группа по умолчанию**. Если в системе создается новый пользователь без указания группы по умолчанию, то такая группа создается автоматически с тем же именем, что и имя пользователя.

Также пользователь может входить в произвольное количество групп, присутствующих в системе. Сведения о них попадают в учетные данные в поле «Дополнительные группы пользователя».



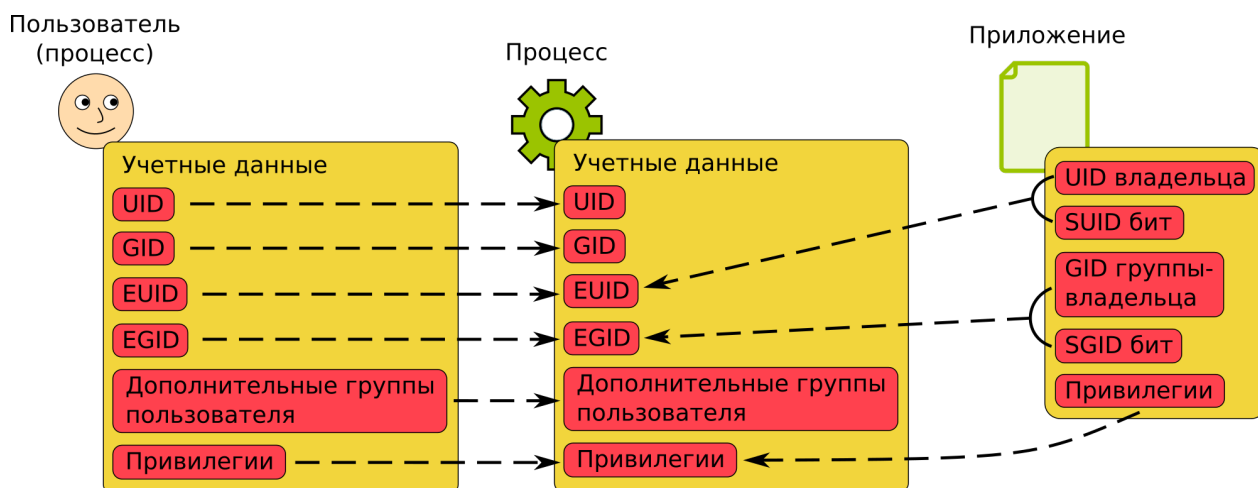


Рис. 36. Схема формирования учетных данных нового процесса. На схеме пользователь запускает приложение, в результате чего стартует новый процесс. Пользователь характеризуется учетными данными так же, как процесс, так как действует посредством другого процесса в ОС. Пунктирные стрелки показывают, какие компоненты учетных данных родительского процесса и атрибутов файла приложения оказывают влияние на формирование определенных компонентов учетных данных дочернего процесса

### 7.1.2. Группы

Каждая группа в Linux, как и пользователь, имеет уникальный целочисленный идентификатор — **group identifier, GID**. Так же, как и для пользователей, присутствует файл `/etc/group`, в котором присутствует информация об имени группы, ее GID и ее членах.

Также стоит обратить внимание на группу с GID равным нулю, это группа по умолчанию суперпользователя. Возможность запуска процесса с таким EGID может привести к полной компрометации системы.

### 7.1.3. Привилегированные программы: биты установки UID и GID

До определенного момента развития Linux в системе не существовало привилегий. Привилегированными процессами считались только те процессы, чей EUID равен нулю. Такие процессы фактически имеют права суперпользователя в системе. Запустить такие процессы может либо сам суперпользователь, либо любой другой пользователь, при условии, что файл запускаемого приложения обладает двумя свойствами:

1. владельцем этого файла является суперпользователь;
2. у файла задан специальный атрибут — **бит установки UID (set UID bit, SUID bit)**.

**SUID бит** — специальный атрибут исполняемого файла приложения, который позволяет осуществляющему выполнение этого приложения процессу изменить EUID на UID владельца исполняемого файла.

Отметим, что совершенно не обязательно, чтобы исполняемый файл принадлежал суперпользователю. Владелец программы может быть любой пользователь системы,

а благодаря SUID биту любой другой пользователь сможет выполнить программу с правами владельца, если другому пользователю в целом будет разрешено выполнение файла.

В ОС Linux присутствует аналогичный атрибут, позволяющий процессам менять EGID на GID группы-владельца файла. Этот атрибут называется **бит установки GID** (**set GID bit**, **SGID bit**). Бит работает аналогично SUID биту, только относительно EGID и GID группы-владельца исполняемого файла, вместо EUID и UID владельца исполняемого файла.

У данного подхода предоставления пользователям возможности выполнить привилегированное действие в системе были очевидные недостатки. Если процессу для своей работы было необходимо выполнить привилегированное действие, то не учитывалось, какое именно действие необходимо произвести процессу, ему сразу давались самые высокие привилегии в системе. При наличии ошибок в таких приложениях с их помощью можно было получить полный контроль над системой. С определенной версии ядра Linux привилегии суперпользователя были разделены на ряд отдельных привилегий.

#### 7.1.4. Привилегии

В текущей версии ядра Linux присутствует 40 привилегий. Описывать все мы не будем, остановимся на некоторых из тех, выполнение процессов с которыми недоверенным пользователем ведет к полной компрометации системы:

- Привилегия **CAP\_SYS\_ADMIN**. Позволяет выполнять множество привилегированных действий в системе: монтировать и демонтировать файловые системы, включать и выключать подкачку, управлять квотами ФС и т. д. Может быть использована злоумышленником для монтирования новой системной ФС и подмены любого системного исполняемого файла или библиотеки.
- Привилегия **CAP\_SYS\_PTRACE**. По сути это привилегия отладки, позволяет контролировать выполнение любого процесса в системе, дает возможность выполнить произвольный код с правами суперпользователя.
- Привилегия **CAP\_SYS\_TTY\_CONFIG**. Позволяет настраивать терминалы. В случае работы в системе терминала под именем суперпользователя позволяет направить в него произвольные команды, что дает возможность выполнить произвольный код с правами суперпользователя.
- Привилегия **CAP\_MKNOD**. Позволяет создавать специальные файлы символьных и блочных устройств. Злоумышленник может использовать обладание этой привилегией для повышения своих прав в системе до максимальных, создав свое блочное устройство на месте системного диска и подменив любой системный исполняемый файл или библиотеку.
- Привилегия **CAP\_SYS\_MODULE**. Позволяет загружать и выгружать модули ядра ОС. Открывает возможность выполнить произвольный код в режиме ядра.
- Привилегия **CAP\_SETFCAP**. Позволяет установить любые привилегии на файл, что ведет к получению любых привилегий при его выполнении.

- Привилегия **CAP\_SETUID**. Позволяет устанавливать произвольный EUID своему процессу. Злоумышленник может использовать эту привилегию, чтобы установить EUID равный нулю для своего процесса и выполнить произвольный код со всеми привилегиями суперпользователя.
- Привилегия **CAP\_CHOWN**. Позволяет менять владельца файла. Злоумышленник может украсть хеши паролей пользователей, задать свои пароли пользователям, считать или записать свои ключи для удаленного доступа пользователей, что приводит к получению прав суперпользователя в системе.

На самом деле около половины всех привилегий позволяют при некоторых сценариях, чаще всего очень простых и актуальных для многих систем, получить полный контроль над системой.

У привилегий Linux есть одно очень существенное отличие от привилегий Windows: в отличие от последних привилегии Linux назначаются на исполняемые файлы, а не даются пользователям системы. Логика та же, что с SUID битом. Разница в том, что раньше вопрос с выполнением привилегированного кода решался запуском исполняемого файла с SUID битом, принадлежащего суперпользователю, что давало приложению все привилегии. Теперь же исполняемый файл

1. не обязательно должен принадлежать суперпользователю и
2. получает в ходе своего выполнения только те привилегии, которые были назначены исполняемому файлу.

Теперь разберемся с последним вопросом относительно привилегий: как процессы и потоки получают свои привилегии:

- Потоки получают те же привилегии, что и главный поток процесса.
- У процессов присутствует 5 наборов привилегий:
  - **Наследуемые** (от англ. «**Inheritable**») — привилегии, которые дочерний процесс может унаследовать.
  - **Разрешенные** (от англ. «**Permitted**») — привилегии, которые поток может использовать.
  - **Эффективные** (от англ. «**Effective**») — текущие (используемые сейчас) привилегии потока.
  - **Ограничивающие** (от англ. «**Bounding**») — набор привилегий, получение которых в дочернем процессе будет ограничено (обсуждается ниже).
  - **Внешние** (от англ. «**Ambient**») — набор привилегий, для предоставления привилегий без использования SUID бита и файловых привилегий.
- У файлов присутствует 2 набора привилегий и один флаг, которые хранятся в расширенном атрибуте «**security.capability**» файла:
  - **Наследуемые** — влияют на наследование привилегий от родительского процесса.
  - **Разрешенные** — влияют на разрешенные привилегии процесса.

- «Флаг эффективности». Если он установлен, то при создании нового процесса его разрешенные привилегии сразу попадут в эффективные.
- Пусть буквой  $P$  обозначается родительский процесс, буквой  $F$  — исполняемый файл, буквой  $P$  со штрихом —  $P'$  — процесс программы  $F$ , запуск которого инициирован процессом  $P$ .  $PI$ ,  $PP$ ,  $PE$ ,  $PB$ ,  $PA$  — наборы привилегий родительского процесса: наследуемые, разрешенные, эффективные, ограничивающие и внешние соответственно.  $P'I$ ,  $P'P$ ,  $P'E$ ,  $P'B$ ,  $P'A$  — аналогичные наборы для процесса  $P'$ .  $FI$ ,  $FP$ ,  $FE$  — наборы наследуемых и разрешенных привилегий файла  $F$  и флаг эффективности соответственно.  $F$  называется привилегированным, если у  $F$  установлены SUID или SGID флаги или назначены привилегии. Тогда наборы процесса  $P'$  формируются по следующим правилам (смотри рисунок 37):
  - Набор  $P'A$  пуст, если файл  $F$  привилегированный, иначе  $P'A = PA$ .
  - Привилегии в наборе  $P'P$  объединяются из трех «слагаемых»:
    - \* Слагаемое 1 формируется из привилегий, которые одновременно присутствуют и в  $PI$ , и в  $FI$ . Те привилегии, которые входят только в  $PI$  или только в  $FI$ , не попадают в Слагаемое 1.
    - \* Слагаемое 2 формируется из привилегий, которые одновременно присутствуют и в  $PB$ , и в  $FP$ . В этом наборе отражен смысл ограничивающего набора родительского процесса: привилегии, которые попадут в разрешенные привилегии дочернего процесса из разрешенных привилегий файла, ограничены привилегиями, которые указаны в ограничивающем наборе родительского процесса.
    - \* Слагаемое 3 равно набору  $P'A$ , определенному на предыдущем шаге.
  - Набор  $P'E$  равен набору  $P'P$ , определенному на предыдущем шаге, если флаг  $FE$  установлен. Иначе набор  $P'E$  равен набору  $P'A$ .
  - Набор  $P'I$  равен набору  $PI$ .
  - Набор  $P'B$  равен набору  $PB$ .

## 7.2. Объекты доступа

ОС Linux придерживается идеологии «все есть файл». И хотя здесь мы будем рассматривать правила доступа к обычным файлам и директориям, эти правила с некоторыми оговорками распространяются на любые объекты ОС: устройства, очереди, сокеты, разделяемые страницы, объекты межпоточковой синхронизации и т. д.

Атрибутами файла, влияющего на доступ к нему, являются:

- **Владелец файла.** При создании файла принимается равным EUID создающего файл процесса. В дальнейшем может быть изменен.
- **Группа-владелец файла.** При создании файла либо принимается равной EGID, либо группе-владельцу родительской директории. В дальнейшем может быть изменена.



с Linux ФС семейства Ext содержат в записях директорий номер **индексного узла** (**index node**, **i-node** — хранилище метаданных о файле), имя файла и тип файла.

- **Запись директории:** возможность создавать и удалять файлы в директории, но необходимо также разрешение на исполнение директории. С точки зрения безопасности довольно опасное право, так как позволяет удалить файлы в директории, не имея никаких прав на эти файлы. Скажем, можно подделать любой файл в директории, сначала удалив его, а затем создав новый с тем же именем.
- **Исполнение директории:** возможность осуществить доступ к файлам внутри директории, в частности прочитать содержимое индексных узлов, а также интерактивно перейти в директорию. Не дает права просмотра имен файлов внутри директории. Тем не менее, доступ к файлу внутри директории может быть осуществлен, если имя файла заранее известно.

### 7.2.2. Биты SUID, SGID и Sticky

Биты SUID и SGID относительно файлов были рассмотрены в подразделе 7.1.3. Относительно директории SUID не имеет эффекта, однако SGID имеет: если SGID установлен на директорию, то группой-владельцем файла, созданного в такой директории, будет являться группа данной родительской директории. В обычном сценарии берется EGID процесса, который создал файл.

**Sticky бит** — атрибут, разрешающий непривилегированному пользователю удалять или переименовывать файлы в директории только в случае, когда соблюдены два условия:

- Пользователь имеет доступ на запись в эту директорию.
- Пользователь является владельцем либо самой директории, либо файла внутри нее, над которым проводится операция удаления или переименования.

Sticky бит является хорошей защитой, когда нужно предоставить возможность создания файлов в директории большому числу пользователей, и в то же время обеспечить защиту от удаления пользователями чужих файлов.

### 7.2.3. Списки управления доступом

Список управления доступом состоит из следующих компонентов (смотри рисунок 38):

- **Запись владельца** — дублирует обычные права владельца файла.
- **Запись группы-владельца** — дублирует обычные права группы-владельца файла.
- **Запись остальных** — дублирует обычные права остальных.
- **Запись пользователя** — запись с тройкой бит, определяющих доступ по базовым правам для произвольного пользователя. Таких записей может быть произвольное число, в том числе такие записи могут отсутствовать.

- **Запись группы** — запись с тройкой бит, определяющих доступ по базовым правам для произвольной группы. Таких записей может быть произвольное число, в том числе такие записи могут отсутствовать.
- **Маска** — запись с тройкой бит, определяет максимальные права, которые могут быть предоставлены из записей группы-владельца, пользователя и группы.

```

права владельца файла
права группы-владельца файла
права остальных
владелец файла
группа-владелец файла

root:~/Documents$ ls -l text.odt
-rw-rw-r--+ 1 root root 7750 Sep  4 14:43 text.odt
root:~/Documents$ getfacl text.odt
# file: text.odt
# owner: root
# group: root
user::rw- запись владельца
user:alice:r-- запись пользователей
user:boris:rw- запись группы-владельца
group::r-- запись групп (одна)
group:users:r-- маска
mask::rw- запись остальных
other::r--
root:~/Documents$

```

Рис. 38. Права файла Linux

На рисунке 38 показаны обычные права и список управления доступом для файла «text.odt». Видим, что владельцем файла является пользователь с именем «root», имя группы-владельца также «root». Владелцу и группе владельца разрешены чтение и запись в файл: когда право не предоставлено, вместо буквы ставится минус, как для права «x» (исполнения) на картинке. Всем остальным пользователям разрешено чтение файла. В списках доступа видим отдельно назначенные права для пользователей alice и boris: первой разрешено чтение, а второму чтение и запись. Также в списках доступа видим, что группе «users» разрешено чтение. Маска говорит о том, что из записей для пользователей и групп можно будет получить права только на чтение и запись, право на исполнение из этих записей получить нельзя.

## 7.3. Авторизация

### 7.3.1. Базовый алгоритм определения правомерности доступа

Этот алгоритм работает, когда у файла не заданы списки управления доступом.

1. Если EUID потока равен нулю, то предоставить любой доступ, кроме доступа на исполнение файла в случае, если флаг исполнения не установлен ни для владельца, ни для группы-владельца, ни для остальных.

2. Если EUID равен UID владельца файла, и права владельца файла перекрывают требуемые права, то предоставить доступ. Иначе запретить.
3. Если EGID или GID одной из дополнительных групп пользователя равен GID группы-владельца, и права группы-владельца файла перекрывают требуемые права, то предоставить доступ. Иначе запретить.
4. Если дошли до этого шага и права остальных файла перекрывают требуемые права, то предоставить доступ. Иначе запретить.

### **7.3.2. Алгоритм определения правомерности доступа для файлов со списком доступа**

1. Если EUID потока равен нулю, то предоставить любой доступ. Как и в шаге 1 алгоритма из подраздела 7.3.1, есть одно исключение: доступ на исполнение запрещается, если ни одна из записей ACL (кроме маски) не содержит права исполнения.
2. Если EUID равен UID владельца файла, то предоставить доступ в соответствии с записью владельца в списке управления аналогично шагу 2 алгоритма из подраздела 7.3.1.
3. Если EUID равен UID в одной из записей пользователей, то предоставить или запретить доступ в соответствии с правами, указанными в записи, за вычетом прав, указанных в маске.
4. Если EGID или GID одной из дополнительных групп пользователя равен GID группы-владельца или GID одной из групп в записях групп, то произвести следующие шаги:
  - а) Если EGID или GID одной из дополнительных групп равен GID группы-владельца и права в записи группы-владельца за вычетом прав, указанных в маске, перекрывают права, необходимые для доступа, то предоставить доступ.
  - б) Если EGID или GID одной из дополнительных групп равен GID одной из записей групп и права в данной записи за вычетом прав, указанных в маске, перекрывают права, необходимые для доступа, то предоставить доступ.
  - в) Если дошли до этого шага, то запретить доступ.
5. Если дошли до этого шага, то предоставить или запретить доступ согласно правам в записи остальных аналогично шагу 4 алгоритма из подраздела 7.3.1.

## **7.4. Аутентификация**

В качестве простого примера аутентификации, разберем работу парольной аутентификации в Linux. Linux хранит хеш-значения паролей на диске в файле `/etc/shadow`. На каждой строчке файла содержится запись, относящаяся к одному пользователю. Запись состоит из значений, разделенных между собой двоеточиями. Опишем эти значения по порядку:

1. **Имя пользователя.**



2. **Хеш-значение пароля пользователя.** Само значение знаками доллара разделено на 3 поля:

- а) **Хеш-функция.** Указывает на то, какая хеш-функция была использована при подсчете хеш-значения пароля. Примеры возможных значений: 1 — соответствует хеш-функции MD-5, 5 — SHA-256, 6 — SHA-512.
- б) **Соль** — случайная строка, присоединяемая к паролю перед вычислением хеш-значения. Усложняет атаки, вычисляющие пароль по хеш-значению с использованием предсчитанных данных. Может быть сформирована база заранее подсчитанных хеш-значений известных паролей, например «admin» или «redfox», которая позволит моментально получать пароль по хеш-значению. Для паролей с солью, например «adminfn84!d» или «redfox3jfd@9», предсчитанного значения в такой базе может не быть, что приведет к невозможности быстрого получения пароля по хеш-значению.
- в) **Хеш-значение пароля.**

- 3. **Дата последнего изменения пароля**, указывается в количестве дней, прошедших с 1 января 1970 года (с этого дня ведет отсчет **время UNIX**).
- 4. **Минимальное время жизни пароля** — число дней, которое должно пройти перед тем, как пароль можно будет сменить. Если не указано, то ноль дней.
- 5. **Максимальное время жизни пароля** — число дней, спустя которое пароль должен быть обязательно сменен. Если не указано, то 99999 дней.
- 6. **Период предупреждения** — число дней перед истечением срока действия паролей, за которое пользователь будет уведомлен об этом.
- 7. **Период неактивности** — число дней после истечения срока действия пароля, по истечении которых учетная запись пользователя будет заблокирована. Если не указано, то пользователь не блокируется.
- 8. **Время жизни учетной записи** — дата по времени UNIX, когда учетная запись будет заблокирована.
- 9. Не используется.

В процессе парольной аутентификации пользователь вводит свои логин и пароль, система проверяет, не заблокирована ли учетная запись и не истек ли срок жизни пароля. Если пользователь не заблокирован и пароль не истек, то к паролю присоединяется соль, от образовавшейся строки вычисляется хеш-значение и сравнивается с хранимым в системе. Если значения совпали, то пользователю разрешен вход.

## 7.5. Вопросы и задания

- 7.1. На основе каких данных субъекта ОС Linux принимает решение о доступе?
- 7.2. Какие права доступа традиционно применяются в ОС Linux?
- 7.3. Для чего служит SUID-бит в ОС Linux?

**7.4.** Что делает маска в списке управления доступом файла в ОС Linux?

**7.5.** Что такое соль хеш-значения пароля в ОС Linux?

**7.6.** Выберите сущности, входящие в учетные данные процесса в ОС Linux:

1. UID пользователя, запустившего процесс.
2. Группы пользователя, запустившего процесс.
3. Привилегии.
4. Права исполняемого файла, из которого был запущен процесс.
5. Флаг эффективности привилегий.

**7.7.** Выберите сущности, входящие в атрибуты безопасности файла в ОС Linux:

1. Тройка прав для каждой группы в системе.
2. Привилегии.
3. Тройка прав владельца файла.
4. Тройка прав пользователей, не являющихся владельцами файла и не входящих в группу владельца файла по умолчанию.
5. Владелец файла.

**7.8.** Выберите сущности, входящие в атрибуты безопасности файла в ОС Linux:

1. Тройка прав для каждой группы в системе.
2. Привилегии.
3. Тройка прав владельца файла.
4. Тройка прав пользователей, не являющихся владельцами файла и не входящих в группу владельца файла по умолчанию.
5. Владелец файла.

**7.9.** Какие наборы привилегий есть у файла в ОС Linux?

**7.10.** Какую хеш-функцию использует ОС Linux для вычисления хеш-значения пароля в ОС Linux?

**7.11.** Что делает конвейер в ОС Linux?

## Список использованной литературы

1. Конституция Российской Федерации [Электронный ресурс]: [принята всенародным голосованием 12.12.1993] (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из справочно-правовой системы «КонсультантПлюс».
2. Уголовный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 13.06.1996 № 63-ФЗ [принят Государственной Думой 24.05.1996] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
3. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.12.2001 № 195-ФЗ [Электронный ресурс]: [принят Государственной Думой 20.12.2001] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
4. Трудовой кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 30.12.2001 № 197-ФЗ [принят Государственной Думой 21.12.2001] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: [принят Государственной Думой 08.07.2006] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]: [принят Государственной Думой 08.07.2006] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
7. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» [Электронный ресурс]: [утверждено Постановлением Правительства Российской Федерации от 03.11.1994 № 1233] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
8. Требования к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [утверждены Постановлением Правительства Российской Федерации от 01.11.2012 № 1119]. Доступ из справочно-правовой системы «КонсультантПлюс».
9. Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами [Электронный ресурс]: [утвержден Постановлением Правительства Российской Федерации от 21.03.2012 № 211] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».

10. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Электронный ресурс]: [утверждено Постановлением Правительства Российской Федерации от 15.09.2008 № 687]. Доступ из справочно-правовой системы «КонсультантПлюс».
11. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных [Электронный ресурс]: [утверждены Постановлением Правительства Российской Федерации от 06.07.2008 № 512] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
12. Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения [Электронный ресурс]: [утверждены приказом Роскомнадзора от 30.05.2017 № 94] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
13. Требования и методы по обезличиванию персональных данных [Электронный ресурс]: [утверждены приказом Роскомнадзора от 05.09.2013 № 996]. Доступ из справочно-правовой системы «КонсультантПлюс».
14. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [утверждены приказом ФСТЭК России от 18.02.2013 № 21] (с изменениями и дополнениями). Доступ из справочно-правовой системы «КонсультантПлюс».
15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) [Электронный ресурс]: [утверждена Заместителем директора ФСТЭК России 15.02.2008]. Доступ из справочно-правовой системы «КонсультантПлюс».
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [утверждена Заместителем директора ФСТЭК России 14.02.2008]. Доступ из справочно-правовой системы «КонсультантПлюс».
17. Состав и содержание 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 [Электронный ресурс]: [утверждены приказом ФСБ России от 10.07.2014 № 378]. Доступ из справочно-правовой системы «КонсультантПлюс».
18. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности [Электронный ресурс]: [утверждены руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432]. Доступ из справочно-правовой системы «КонсультантПлюс».

19. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]: Доступ из справочной системы «ТЕХЭКСПЕРТ».
20. Таненбаум, Э. Архитектура компьютера. 6-е изд. / Э. Таненбаум, Т. Остин. СПб.: Питер, 2019. 816 с.
21. Таненбаум, Э. Операционные системы. Разработка и реализация. 3-е изд. / Э. Таненбаум, А. Вудхалл. СПб.: Питер, 2007. 704 с.
22. Таненбаум, Э. Современные операционные системы. 4-е изд. / Э. Таненбаум, Х. Бос. СПб.: Питер, 2015. 1120 с.
23. Фленов, М. Е. Linux глазами хакера. 5-е изд. / М. Е. Фленов. СПб.: БХВ-Петербург, 2019. 416 с.
24. Лав, Р. Linux. Системное программирование. 2-е изд. / Р. Лав. СПб.: Питер, 2014. 448 с.
25. Уорд, Б. Внутреннее устройство Linux / Б. Уорд. СПб.: Питер, 2016. 384 с.
26. Yosifovich, P. Windows Internals Seventh Edition. Part 1 / P. Yosifovich, A. Ionescu, M. E. Russinovich, D. A. Solomon. Microsoft Press, 2017. 784 p.
27. Intel 64 and IA-32 Architectures Software Developer's Manual [Электронный ресурс]: электрон. текстовые дан. Дата обновления: 16.11.2020. URL: <https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html> (дата обращения: 16.11.2020).
28. Принцип продольной (сверху) и перпендикулярной (снизу) записи [Электронный ресурс]: Дата обновления: 21.06.2005. URL: <http://commons.wikimedia.org/w/index.php?title=File:Perpendicular-eng.jpg> (дата обращения: 16.11.2020).

Учебное издание

Князев Владимир Николаевич

Мурин Дмитрий Михайлович

# БЕЗОПАСНОСТЬ В СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ СРЕДЕ

Часть 1

*Учебное пособие*

Редактор, корректор А. А. Аладьева

Компьютерный набор и верстка В. Н. Князев, Д. М. Мурин.

Подписано в печать 29.01.2021. Формат 60 × 84 <sup>1</sup>/<sub>8</sub>.

Усл. печ. л. 17,67. Уч.-изд. л. 13,3.

Тираж 64 экз. Заказ 025-2021.

Оригинал-макет подготовлен авторами.

Ярославский государственный университет им. П. Г. Демидова.  
150003, Ярославль, ул. Советская, 14.

ООО «Издательско-полиграфический комплекс «ИНДИГО».  
150049, Ярославль, ул. Свободы, 97.  
E-mail: info@indigo-press.ru

Отпечатано на собственном полиграфическом оборудовании.