

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского
федерального университета
Дата подписания: 23.08.2023 15:53:26
Уникальный программный ключ:
d74ce93cd40e39275c3ba2f58486412a1c8ef96f

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания
по выполнению практических работ
по дисциплине
**«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ»**
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

**Пятигорск
2022**

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

ВВЕДЕНИЕ

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Организационно-правовое обеспечение информационной безопасности» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по правовому регулированию отношений в информационной сфере, по обеспечению защиты сведений ограниченного доступа от утечки по техническим каналам, разглашения, несанкционированного доступа на объектах информатизации и в выделенных помещениях, а также по формированию навыков работы в области защиты информации.

Задачами дисциплины являются:

1. Ознакомление с основами правового регулирования отношений в информационной сфере;
2. Ознакомление с конституционными гарантиями прав граждан на получение информации и механизмом их реализации,
3. Изучение понятий и видов защищаемой информации по законодательству РФ,
4. Изучение системы защиты государственной тайны,
5. Ознакомление с основами правового регулирования отношений в области интеллектуальной собственности; способами защиты этой собственности,
6. Изучение понятия и видов компьютерных преступлений;
7. Обучение основам организации обеспечения защиты информации на объектах информатизации и в выделенных помещениях;
8. Формирование практических навыков работы в области защиты информации.

2. Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
6 семестр			
1	Практическая работа №1. Предмет информационного права в информационной безопасности	3	
2	Практическая работа №2. Общая характеристика законодательства Российской Федерации в области информационной безопасности	3	
3	Практическая работа №3. Правовое обеспечение защиты государственной тайны	1,5	
4	Практическая работа №4. Система защиты государственной тайны	3	
5	Практическая работа №5. Правовое обеспечение защиты банковской, профессиональной и служебной тайны	1,5	
6	Практическая работа №6. Правовое обеспечение защиты профессиональной и служебной тайны	3	
7	Практическая работа №7. Правовое обеспечение защиты коммерческой тайны	3	

8	Практическая работа № 8 Правовое обеспечение защиты персональных данных	3	
9	Практическая работа № 9. Правовое обеспечение защиты интеллектуальной собственности	3	
	Итого за 6 семестр	24	
7 семестр			
1	Практическая работа № 1. Предмет информационного права в информационной безопасности	3	
2	Практическая работа № 2. Система обеспечения информационной безопасности	3	
3	Практическая работа № 3. Организационные структуры системы обеспечения безопасности информации	3	
4	Практическая работа № 4. Разработка модели информационных потоков предприятия (организации) с использованием программного комплекса гриф-2006	3	
5	Практическая работа № 5. Организация режимов безопасности	3	
6	Практическая работа № 6. Организация работы с персоналом	3	
7	Практическая работа № 7. Исследование юридической ответственности	3	
8	Практическая работа № 8. Борьба с компьютерными преступлениями	1,5	
9	Практическая работа № 9. Борьба с компьютерными преступлениями	1,5	
10	Практическая работа № 10. Организация защиты прав	1,5	
11	Практическая работа № 11. Организация защиты прав	1,5	
	Итого за 7 семестр	27	
	Итого	51	

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1-2.1.-2.

Предмет: Информационное право в информационной безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Право – это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Законодательство Российской Федерации представляет собой совокупность Конституции и принимаемых в соответствии с ней законов и подзаконных актов.

Внутреннее строение системы права РФ можно представить в вертикальном и горизонтальном срезах.

Вертикальное строение права – совокупность элементов, включающих: отрасль, подотрасль, институт, субинститут и правовое предписание.

Горизонтальное строение права позволяет увидеть все отрасли, его составляющие. Если их классифицировать, то можно выделить две группы отраслей.

В первую группу объединяются **регулятивные отрасли права**, т. е. отрасли, в которых основной упор делается на установление прав и обязанностей участников правоотношений.

Вторую группу отраслей составляют **охранительные отрасли права**, основной задачей которых является защита правоотношений.

Структура правоотношений и виды юридической ответственности

Правоотношение – это такое общественное отношение, в котором стороны связаны между собой взаимными юридическими правами и обязанностями, охраняемыми государством. Правоотношение есть та мера

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

внешней свободы, которая предоставляется его участникам нормами позитивного (писаного) права.

Структура правового отношения имеет четыре необходимых элемента: субъекты, объект, право и обязанность:

Субъекты правоотношений – это отдельные индивиды и организации, которые в соответствии с нормами права являются носителями юридических прав и обязанностей. В реальной жизни не все индивиды и организации могут быть субъектами правоотношений, например, малолетние дети, душевнобольные, организации, прекратившие свое существование, фактически не могут участвовать в правоотношениях по понятным причинам.

Мера участия субъектов в правовых отношениях определяется их правоспособностью и дееспособностью.

Правоспособность – это способность субъекта иметь юридические права и нести юридические обязанности. Она начинается с момента рождения индивида и прекращается смертью. Однако чтобы стать реальным участником правоотношения, правоспособный субъект должен быть дееспособным.

Дееспособность – это способность субъекта самостоятельно, своими действиями осуществлять юридические права и нести обязанности.

1. Объект правоотношений – это то, на что воздействует правоотношение.

Объектом правоотношения является фактическое поведение его участников. В соответствии с содержанием субъективного права и юридической обязанности участники правоотношения строят свое поведение. Вступая в правоотношения, субъекты удовлетворяют определенные материальные, духовные и иные потребности (например, приобретают вещи, пользуются авторскими правами, правами изобретателя). Объектом правоотношений выступает поведение людей, которое может быть различным по содержанию.

2. Субъективное право – это предоставляемая и охраняемая государством возможность (свобода) субъекта по своему усмотрению удовлетворять те интересы, которые предусмотрены позитивным правом. Право, принадлежащее субъекту, называется субъективным потому, что только от воли субъекта зависит, как им распорядиться. Это возможность не произвольная, а правовая, устанавливающая меру дозволенного поведения.

3. Юридическая обязанность – это предусмотренная законодательством и охраняемая государством необходимость должного поведения участника правового отношения в интересах управомоченного субъекта (индивида, организации, государства в целом). Если содержание субъективного права образует мера дозволенного поведения, то содержание обязанности – мера

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

должного, необходимого поведения в правоотношении.

Юридическая ответственность – это применение к правонарушителю предусмотренных санкцией юридической нормы мер государственного принуждения, выражающихся в форме лишений личного, организационного либо имущественного характера. Фактическим основанием для юридической ответственности является правонарушение. Лицо может быть привлечено к ответственности только при наличии в его действии всех элементов состава правонарушения.

Состав правонарушения состоит из четырех составляющих:

- **объект правонарушения** – область общественных отношений, регулируемых и охраняемых правом, в котором произошло деяние и (или) которой данным деянием причинен вред;
- **объективная сторона** – характеристика деяния, способа его совершения (группой, с применением оружия, систематически, повторно), обстоятельств (во время военных действий, стихийных бедствий и т. п.);
- **субъект** – лицо, которое совершило правонарушение, характеристика правонарушителя;
- **субъективная сторона** – форма вины (умысел или неосторожность).

Само по себе правонарушение не порождает автоматически возникновения ответственности, а является лишь основанием для такого применения. Для реального же осуществления юридической ответственности необходим **правоприменительный акт** – решение компетентного органа, который возлагает юридическую ответственность, устанавливает объем и форму принудительных мер к конкретному лицу. Это может быть приговор суда, приказ администрации и т. п. Наибольшее распространение получило деление юридической ответственности по отраслевому признаку. По данному основанию различают ответственность уголовную, административно-правовую, гражданско-правовую, дисциплинарную и материальную.

Уголовная ответственность наступает за совершение преступлений и в отличие от других видов ответственности устанавливается только уголовным законом. Никакие иные нормативные акты не могут определять общественно опасные деяния как преступные и устанавливать за них меры ответственности. В Российской Федерации исчерпывающий перечень преступлений зафиксирован в Уголовном кодексе. Порядок привлечения к уголовной ответственности регламентируется Уголовно-процессуальным кодексом. Полномочиями привлечения к уголовной ответственности обладает только суд.

Административно-правовая ответственность наступает за совершение административных проступков, предусмотренных Кодексом об административных правонарушениях. Кроме того, этот вид ответственности может устанавливаться указами Президента Российской Федерации, постановлениями Правительства Российской Федерации и нормативными актами субъектов Федерации. Дела об административных правонарушениях рассматриваются компетентными органами государственной власти, круг которых закреплен в кодексе. Меры административного принуждения – предупреждение, штраф, лишение специального права, административный арест.

Гражданско-правовая ответственность наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. Ее сущность состоит в принуждении лица нести отрицательные имущественные последствия. Полное возмещение вреда – основной принцип гражданско-правовой ответственности (статья 1064 ГК). Возмещение убытков в некоторых случаях дополняется штрафными санкциями, например, выплатой неустойки.

Дисциплинарная ответственность возникает вследствие совершения дисциплинарных проступков. Привлекать к дисциплинарной ответственности может руководитель, осуществляющий распорядительно-дисциплинарную власть над конкретным работником. Меры дисциплинарной ответственности – выговор, строгий выговор, отстранение от занимаемой должности и т. п.

Материальная ответственность рабочих и служащих за ущерб, нанесенный предприятию, учреждению, заключается в необходимости возместить ущерб в порядке, установленном законом. Основанием этого вида ответственности является нанесение ущерба во время работы предприятию, с которым работник находится в трудовых отношениях. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

Информационное законодательство – это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предметом правового регулирования в информационной сфере являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация права на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

- создание и применение средств информационной безопасности.

В целях реализации этих прав и свобод принимаемые законодательные акты устанавливают гарантии, обязанности, механизмы защиты и ответственность.

Информационное законодательство имеет вертикальную (по видам правовых актов) и горизонтальную (по отраслям законодательства) структуру.

Вертикальная структура строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются определяющими для соответствующих норм всех нижестоящих актов.

Структура информационного законодательства как комплексной отрасли включает в себя:

- Международные акты информационного законодательства.
- Информационно-правовые нормы Конституции РФ.
- Отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства.
- Отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

Совокупность вышеперечисленных документов составляет правовую базу, обеспечивающую нормативное регулирование процессов информационного обмена, в том числе и защиту информации.

Информация имеет ряд особенностей, отличающих ее от других видов товаров:

- нематериальность (идеальность) информации;
- информационный продукт подвергается только моральному износу;
- информация находится на материальном носителе;
- информация не исчезает при потреблении и может быть использована многократно;
- производство информации требует значительных затрат по сравнению с затратами на тиражирование;
- при копировании количество информации не изменяется, а цена снижается.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Основные определения в области информационного права:

Информация – это сведения о лицах, предметах, фактах, явлениях, процессах независимо от формы их представления.

Документированная информация – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Объект правоотношений – это то, на что воздействуют правоотношения.

Субъект правоотношений – предоставленная и охраняемая государством возможность субъекта по своему усмотрению удовлетворять потребности, предусмотренные позитивным правом.

Юридическая ответственность – применение предусмотренных санкций, юридических норм, мер государственного принуждения.

Юридические обязанности – предусмотренная законодательством и охраняемая государством необходимость должностного поведения участника правоотношений.

Правовые принципы защиты информации:

- полнота правового регулирования;
- принципы единства нормативно-правовой базы;
- непротиворечивость законодательной базе;
- принцип соблюдения рациональных пропорций между правовыми и технико-юридическими нормами;
- нормативно-правовые акты должны предусматривать развернутую защиту прав граждан.

Контрольные вопросы

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?

6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3-4.

Общая характеристика законодательства российской федерации в области информационной безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В настоящее время с учетом сложившейся практики обеспечения информационной безопасности принято выделять следующие направления защиты информации:

- правовая защита – это специальные законы и другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

Правовое обеспечение информационной безопасности любой страны содержит как международные, так и национальные правовые нормы. В нашей стране правовые или законодательные основы обеспечения информационной безопасности составляют Конституция РФ, Законы РФ, Кодексы, Указы и другие нормативные акты, регулирующие отношения в области информации.

Правовая защита информации как ресурса признана на международном уровне и определяется межгосударственными договорами, конвенциями, декларациями, реализуется правовыми механизмами защиты патентных и авторских прав.

В реализации государственной политики в сфере информатизации участвуют следующие структуры власти:

- Президент Российской Федерации;
- Совет Федерации;

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

- Государственная дума Федерального собрания Российской Федерации;
- Правительство Российской Федерации;
- Совет безопасности Российской Федерации;
- федеральные органы исполнительной власти;
- органы государственной власти Российской Федерации;
- органы местного самоуправления.

Совет безопасности Российской Федерации рассматривает наиболее важные вопросы, связанные с безопасностью Российской Федерации в современном мире, в том числе и вопросы информационной безопасности.

Структуру аппарата системы безопасности Российской Федерации составляют:

- Управление информационной безопасности и стратегического прогнозирования;
- Межведомственная комиссия Совета безопасности Российской Федерации по информационной безопасности.

В Государственной думе Российской Федерации функционируют:

- Комитет по информационной политике и связи;
- Комитет по безопасности, составной частью которого является комитет по информационной безопасности.

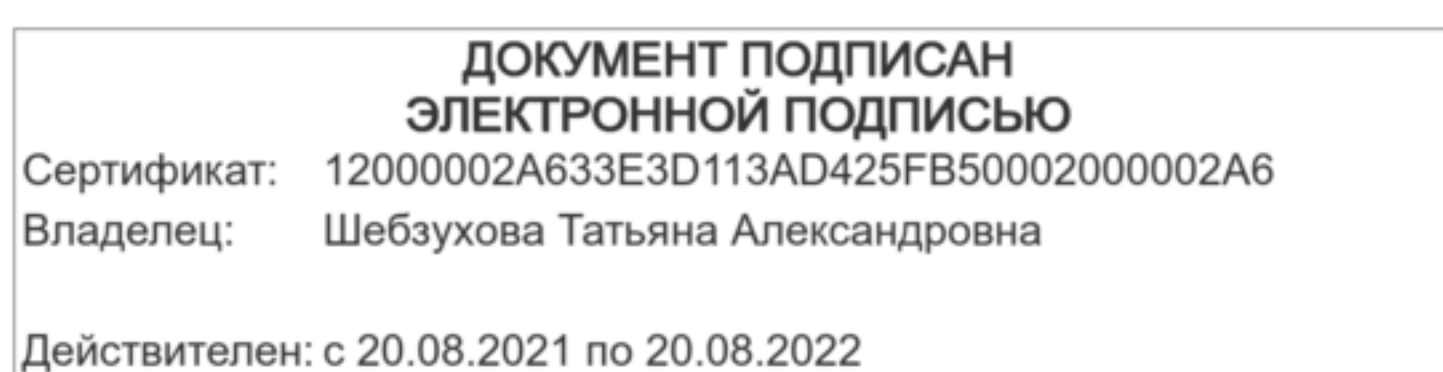
На внутригосударственном уровне правовая защита регулируется государственными и ведомственными актами. Государственными актами являются Конституция РФ, законы РФ, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями.

Информационное законодательство — совокупность норм права, регулирующих общественные отношения в информационной среде.

Предметом правового регулирования в информационной среде являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация прав граждан на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

Таким образом, законодательство по информационной безопасности является неотъемлемой частью всей системы законов Российской Федерации.



Федеральный закон «Об информации, информационных технологиях и о защите информации»

Со дня вступления в силу Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» утратили силу Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» и Федеральный закон от 04 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене».

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:

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

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Термины, используемые в законе, их определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

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.

Доступ к информации – возможность получения информации и ее использования.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации – действия, направленные на получение

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством

Российской Федерации случаях ее материальный носитель.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Важнейшие задачи обеспечения информационной безопасности Российской Федерации:

1. Противодействие угрозе развязывания противоборства в информационной сфере.
2. Реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности.
3. Совершенствование и защита отечественной информационной структуры, интеграция России в мировое информационное пространство.

Доктрина информационной безопасности РФ развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и служит основой для:

- 1) формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- 2) подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- 3) разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Под *информационной безопасностью Российской Федерации* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

создаваемых на территории России.

Федеральный закон «О техническом регулировании»

Федеральный закон «О техническом регулировании» от 27 декабря 2002 года № 184-ФЗ регулирует отношения, возникающие при:

- 1) разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- 2) разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- 3) оценке соответствия продукции установленным законодательством требованиям.

Требования к функционированию единой сети связи Российской Федерации и к продукции, связанные с обеспечением целостности, устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

Действие закона не распространяется на государственные образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг.

Термины, используемые в законе, их определения

Аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

Безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов.

Декларация о соответствии – документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

Заявитель – физическое или юридическое лицо, осуществляющее обязательное подтверждение соответствия.

Знак обращения на рынке – обозначение, служащее для информирования приобретателей о соответствии выпускаемой в обращение продукции требованиям технических регламентов.

Знак соответствия – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

Идентификация продукции – установление тождественности характеристик продукции ее существенным признакам.

Контроль (надзор) за соблюдением требований технических регламентов – проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки.

Международный стандарт – стандарт, принятый международной организацией.

Национальный стандарт – стандарт, утвержденный национальным органом Российской Федерации по стандартизации.

Орган по сертификации – юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации.

Оценка соответствия – прямое или косвенное определение соблюдения требований, предъявляемых к объекту.

Подтверждение соответствия – документальное удостоверение соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Продукция – результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях.

Риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда.

Сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Сертификат соответствия – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

Система сертификации – совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом.

Стандарт – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Стандартизация – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Техническое регулирование – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия.

Технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

Форма подтверждения соответствия – определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Закон Российской Федерации «О безопасности»

Закон РФ «О безопасности» от 5 марта 1992 года № 2446-1 закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Термины, используемые в законе, их определения

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся:

- 1) личность – ее права и свободы;
- 2) общество – его материальные и духовные ценности;
- 3) государство – его конституционный строй, суверенитет и территориальная целостность.

Субъект обеспечения безопасности – государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей. Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности.

Принципы обеспечения безопасности

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

Контрольные вопросы

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?
6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.
12. Назовите и охарактеризуйте направления защиты информации.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5-6.

Правовое обеспечение защиты государственной тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Информация ограниченного доступа, включающая государственную тайну и конфиденциальную информацию, имеет особую важность для государства и общества. В той или иной мере правовые институты тайн есть во всех развитых демократиях мира.

Опыт показывает, что с ростом значимости информации в общей системе государственного и муниципального управления (ГМУ) наиболее важным элементом с годами становится достижение превосходства в информационной сфере. Этим обстоятельством и определяется существование институтов тайн, создающих возможность для ГМУ проводить независимую информационную политику, защищать свои интересы, осуществлять управление обществом, регионом, муниципальным образованием.

Система секретной и конфиденциальной информации – наиболее сильное звено регулирования общественных отношений в информационной сфере. Вследствие возможного существенного ущерба от ее разглашения информация ограниченного доступа занимает особое место в системе управления. Институт тайн – важнейший элемент системы государственного и муниципального управления.

Основу нормативно-правового обеспечения защиты информации ограниченного доступа в России составляют Конституция РФ, законы

«О безопасности» от 5 марта 1992 года № 2446-1, «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ и другие.

В условиях сегодняшней России (расширяющееся международное сотрудничество, либерализация экономики, увеличение количества объектов иностранных инспекций, свободное перемещение иностранцев по большей части территории страны, внедрение компьютерной техники иностранного производства) значительной возросла опасность утечки сведений, составляющих информацию

ограниченного доступа. В связи с этим в настоящее время одной из важнейших задач органов ГМУ являются обеспечение безопасности государственного и муниципального баланса между потребностью в свободном распространении информации и ее ограничением на ее распространение, а также развитие и защита государственного и муниципального ресурса.

В действующем законодательстве РФ встречается упоминание более чем о

ограниченного доступа. В связи с этим в настоящее время одной из важнейших задач органов ГМУ являются обеспечение безопасности государственного и муниципального баланса между потребностью в свободном распространении информации и ее ограничением на ее распространение, а также развитие и защита государственного и муниципального ресурса.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

30 видах различных тайн (государственная, служебная, коммерческая, банковская, личная, семейная, тайна следствия, связи, почтовых отправлений и другие).

Приведем наиболее важные определения в этой области и дадим необходимую классификацию.

Защищаемой информацией называется информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. К защищаемой информации относится информация с ограниченным доступом, а также открытая информация, представляющая ценность.

Информацией с ограниченным доступом называется информация, доступ к которой ограничен в соответствии с Законом с целью защиты прав и законных интересов субъектов права на тайну. Она состоит из государственной тайны и конфиденциальной информации.

Конфиденциальная информация в свою очередь включает множество видов тайны, которые сводятся к шести основным видам:

- 1) персональные данные;
- 2) тайна следствия и судопроизводства;
- 3) служебная тайна;
- 4) профессиональная тайна;
- 5) коммерческая тайна;
- 6) тайна изобретения, полезной модели и промышленного образца.

Особую важность с точки зрения безопасности государства имеет защита информации, составляющей государственную и служебную тайну.

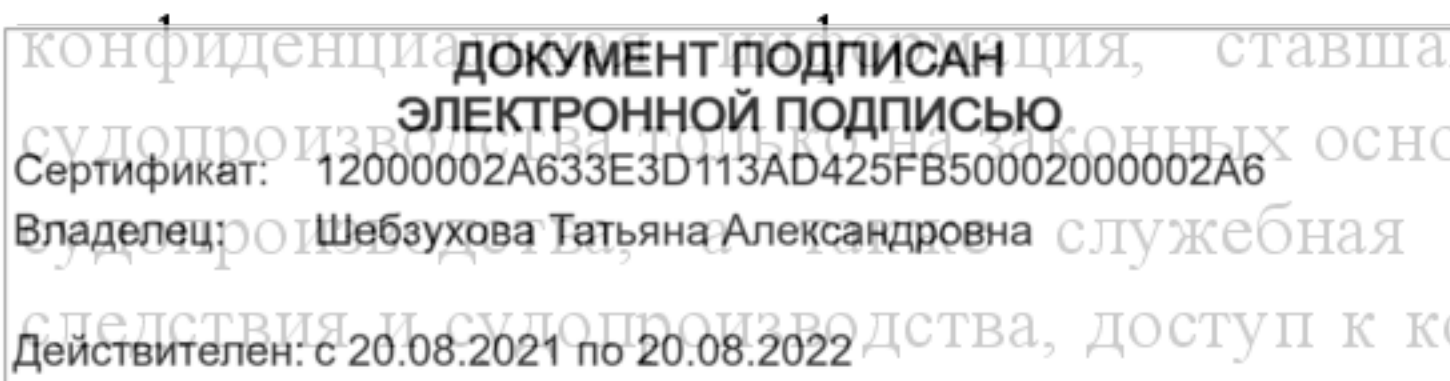
Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Конфиденциальная информация – информация, не составляющая государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Тайна следствия и судопроизводства – защищаемая по закону информация, ставшая известной в органах следствия и судопроизводства на законных основаниях в ходе следствия и информации о деятельности органов следствия и судопроизводства, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна – защищаемая по закону конфиденциальная



информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, банковская тайна и т. д.).

Коммерческая тайна – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности меры охраны.

Тайна изобретения, полезной модели или промышленного образца – сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Согласно законодательству обязательными признаками информации с ограниченным доступом должны быть:

1. Информация имеет действительную или потенциальную ценность для ее обладателя в силу неизвестности ее третьим лицам. Таковыми лицами могут быть государство, юридические или физические лица.
2. К информации нет свободного доступа на законном основании.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Возможность сохранения ее неизвестной для третьих лиц установлена законом.

3. Обладатель информации принимает меры по ее защите.

К государственной тайне относятся сведения, удовлетворяющие следующим признакам:

1. Сведения в строго установленных сферах деятельности государства (военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно розыскной деятельности) и ни в каких других.
2. Сведения, не известные широкому, точнее – неопределенному неконтролируемому кругу лиц, и представляющие ценность именно в силу такой неизвестности.
3. Сведения, распространение которых может нанести ущерб безопасности РФ. При этом величина ущерба такова, что влияет на безопасность государства.
4. Сведения, относительно которых предпринимаются специальные меры защиты, направленные на предотвращение их неконтролируемого распространения.

Система документов по защите государственной тайны

Документы по защите государственной тайны по функционально-целевому назначению подразделяются на следующие основные классы:

- нормативные правовые;
- организационно-распорядительные;
- нормативные;
- плановые;
- информационные.

Нормативные правовые акты в области защиты государственной тайны включают:

- федеральные законы;
- указы и распоряжения Президента РФ;
- постановления и распоряжения высших органов исполнительной и судебной властей РФ.

Базовыми законами в области защиты государственной тайны являются специальные законы «О государственной тайне» от 21 июля 1993 года

№ 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, а также нормативные правовые акты более общего характера: Конституция РФ, Гражданский и Уголовный кодексы РФ и др.

На их основе **организационно-распорядительные документы**

определяют состав и регламентируют деятельность соответствующих органов и служб при организации и осуществлении защиты государственной тайны. Эти

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

документы по характеру регламентируемых вопросов (решаемых задач) и продолжительности действия подразделяют на два вида:

- основополагающие (руководящие) документы;
- распорядительные документы (документы оперативного управления).

Основополагающие (руководящие) документы помимо самостоятельного использования служат основой при разработке нормативных, плановых и информационных документов. Они являются подзаконными актами, детализирующими и раскрывающими положения нормативных правовых актов, и устанавливают основные направления, единые принципы, порядок организации защиты государственной тайны соответствующими органами и службами с приведением их задач, функций, прав, обязанностей и мер ответственности.

Положения по защите государственной тайны издаются на основе нормативных правовых актов и принятых концепций и детализируют указные документы, в основном по вопросам организации защиты государственной тайны в конкретном органе государственной власти (ведомстве) и, в частности, регламентируют:

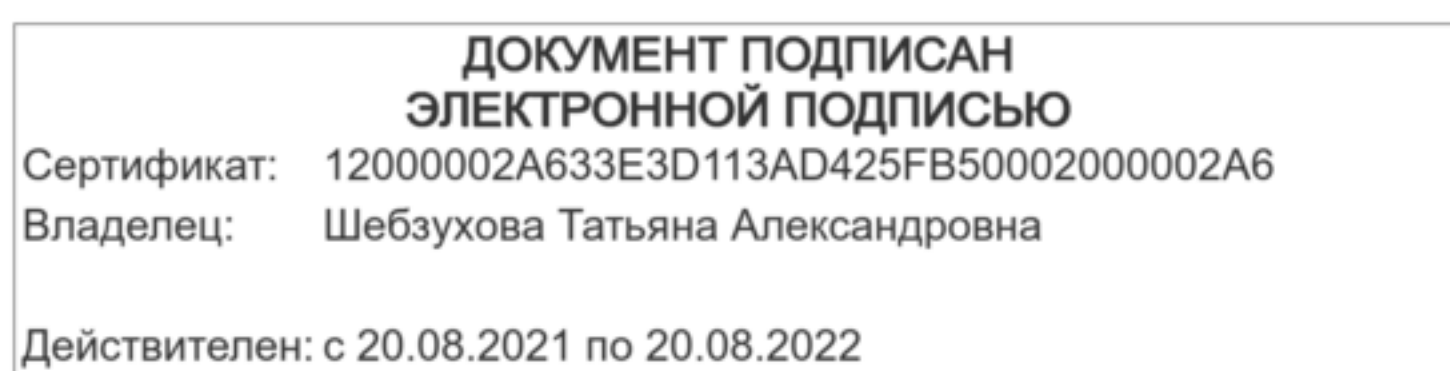
- основные направления работ по защите государственной тайны;
- структуру органов и служб, ответственных за организацию и осуществление защиты государственной тайны, их права и обязанности;
- порядок организации и проведения типовых работ по защите государственной тайны для основных объектов защиты;
- финансово-экономические вопросы обеспечения работ по защите государственной тайны;
- вопросы государственного лицензирования в области защиты государственной тайны.

Детальные разъяснения отдельных практических вопросов по организации и осуществлению защиты государственной тайны включаются в соответствующие руководства, наставления, инструкции и правила.

Распорядительные документы – документы текущего (оперативного) управления издают во исполнение или в дополнение к основополагающим документам. Основными видами распорядительных документов по защите государственной тайны являются решения, приказы, директивы, распоряжения, указания.

Нормативные документы устанавливают единые требования, нормы и правила защиты информации, составляющей государственную тайну, обязательные для исполнения в пределах установленной при их введении сферы действия и области их распространения.

Основными видами нормативных документов, в которых



регламентируются вопросы защиты государственной тайны, являются:

- специальные нормативные документы федеральных органов исполнительной власти, ответственных за обеспечение защиты государственной тайны;
- нормативные документы государственной системы стандартизации. К специальным нормативным документам относятся:
- требования и нормы по защите государственной тайны;
- методики проведения работ в области защиты государственной тайны;
- лицензии предприятиям на право осуществления работ в области защиты государственной тайны;
- сертификаты соответствия средств защиты информации;
- аттестаты на объекты защиты.

Плановые документы включают целевые программы и планы в области защиты государственной тайны или соответствующие разделы программ и планов более общего характера, по которым осуществляется самостоятельное финансирование.

Информационные документы служат для информационного обеспечения решения задач организации и осуществления защиты государственной тайны.

По форме представления информационные документы могут быть следующих видов:

- справочные документы;
- отчетная научно-техническая документация;
- учебная и научная литература;
- формы документов служебного делопроизводства.

Федеральный закон «О государственной тайне»

Положения федерального закона «О государственной тайне» от 21 июля 1993 года № 5485-1 обязательны для исполнения на территории Российской Федерации и за ее пределами органами *законодательной*, исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Термины, используемые в законе, их определения

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной,

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Носители сведений, составляющих государственную тайну –

материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов сигналов, технических решений и процессов.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а также предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Правовой режим защиты государственной тайны

Перечневый подход к организации защиты государственной тайны

В настоящее время в России существуют как открытые, так и закрытые перечни сведений. Открытыми перечнями являются приведенный в Законе «О государственной тайне» перечень сведений, составляющих государственную тайну, а также утверждаемый Указом Президента РФ перечень сведений, отнесенных к государственной тайне. Кроме того, существуют ведомственные перечни сведений, подлежащих засекречиванию, которые могут быть как открытыми, так и закрытыми.

С их помощью реализуется подход к организации защиты государственной

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

тайны в виде системы перечней, включающей:

- перечень сведений, составляющих государственную тайну (определен в Законе «О государственной тайне»);
- перечень сведений, отнесенных к государственной тайне (утверждается Указом Президента РФ);
- развернутый перечень сведений, подлежащих засекречиванию в органе государственной власти (утверждается руководителями органов власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне);
- перечни сведений, подлежащих засекречиванию, на предприятии, в учреждении и организации (представляют собой выписки из развернутых перечней сведений, подлежащих засекречиванию).

Перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом «О государственной тайне», руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделяемых полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Перечень не закрепощает набор конкретных сведений путем прямого отнесения их к государственной тайне, а лишь создает законодательную базу для отнесения конкретных сведений к государственной тайне, если для этого имеется соответствующее обоснование. Такой подход должен позволить системе засекречивания адаптироваться к динамичному развитию нашего общества, ослабить искусственную секретность, наносящую ущерб экономическим интересам РФ.

Установлена персональная ответственность конкретных должностных лиц за принятие решения по отнесению сведений к государственной тайне. Именно за ними сохраняется ответственность за обоснованность, в том числе экономическую, установленной степени секретности конкретных сведений. Именно на них возложена функция гибкого и своевременного реагирования на внешние условия изменения режима секретности, чтобы последний не превращался в фактор, тормозящий развитие экономики, науки и межгосударственных отношений.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- 1) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- 2) о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- 3) о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- 4) о фактах нарушения прав и свобод человека и гражданина;
- 5) о размерах золотого запаса и государственных валютных резервах РФ;
- 6) о состоянии здоровья высших должностных лиц РФ;
- 7) о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Контрольные вопросы

1. Перечислите основные виды тайн. Охарактеризуйте каждый вид.
2. Назовите обязательные признаки информации с ограниченным доступом.
3. На какие классы по функциональному назначению подразделяются документы по защите государственной тайны?
4. Дайте определение понятию «гриф секретности».
5. Какие сведения не относятся к государственной тайне и не подлежат засекречиванию?
6. Перечислите органы защиты государственной тайны.
7. Какие существуют методы защиты сведений, составляющих государственную тайну?
8. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7-8.

Система защиты государственной тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны), Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне.

Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом РФ.

Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны,

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

Служба внешней разведки РФ, Государственная техническая комиссия при президенте РФ и их органы на местах организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции.

Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Защита государственной тайны является основным видом деятельности органов государственной власти, предприятий, учреждений или организаций.

Цель защиты государственной тайны заключается в предотвращении или снижении величины ущерба безопасности государства путем исключения (существенного затруднения) утечки информации по всем возможным каналам.

Методы защиты сведений, составляющих государственную тайну, подразделяются на правовые, организационно-технические и экономические.

К **правовым методам** обеспечения защиты сведений, составляющих государственную тайну, относится разработка нормативных правовых актов, регламентирующих отношения в области защиты государственной тайны, и нормативных методических документов по вопросам обеспечения защиты государственной тайны.

Организационно-техническими методами обеспечения защиты сведений, составляющих государственную тайну, являются:

- создание и совершенствование системы защиты государственной тайны в РФ;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, включая предупреждение и пресечение правонарушений в области защиты государственной тайны, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств

информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно- телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;
- формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах жизни и деятельности общества и государства, в том числе и по вопросам обеспечения защиты государственной тайны.

Экономические методы обеспечения защиты государственной тайны включают в себя:

- разработку федеральных программ в области защиты государственной тайны и определение порядка их финансирования;
- установление и наложение штрафов на должностных и юридических лиц за нарушения требований по защите государственной тайны.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов:

- бумажные документы;
- магнитные носители информации в электронно-вычислительных машинах;
- электромагнитные поля, создаваемые радиоэлектронными средствами при передаче информации;
- физические проявления объектов (органов управления, промышленных предприятий и др.), сведения о которых составляют государственную тайну, в виде разнообразных полей и следов деятельности.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Как носители сведений в современных условиях особую роль имеют технические средства сбора, передачи, хранения и обработки информации. С их использованием обрабатывается основной объем информации, составляющей государственную тайну. Их недостатком является уязвимость для широкого спектра угроз несанкционированного распространения защищаемой информации. Защите информации на таких носителях уделяется особое внимание.

Человек в действующем Законе РФ «О государственной тайне»

не рассматривается как специфический носитель сведений, хотя он в своей памяти может хранить эти сведения. Тем самым человек не ставится на один уровень с техническими носителями. Он в проблеме защиты государственной тайны рассматривается как субъект общественных отношений, возникающих в процессе защиты государственной тайны.

Полномочия органов государственной власти и должностных лиц в области защиты государственной тайны

Палаты Федерального собрания:

- осуществляют законодательное регулирование отношений в области государственной тайны;
- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
- определяют полномочия должностных лиц в аппаратах палат Федерального собрания по обеспечению защиты государственной тайны.

Президент РФ:

- утверждает государственные программы в области защиты государственной тайны;
- утверждает по представлению Правительства РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства РФ перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также перечень сведений, отнесенных к государственной тайне;
- заключает международные договоры РФ о совместном использовании и защите сведений, составляющих государственную тайну;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента РФ;
- в пределах своих полномочий решает иные вопросы, возникающие в

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

Правительство РФ:

- организует исполнение Закона РФ «О государственной тайне» ;
- представляет на утверждение Президенту РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает порядок разработки Перечня сведений, отнесенных к государственной тайне;
- организует разработку и выполнение государственных программ в области защиты государственной тайны;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства РФ;
- устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;
- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
- заключает межправительственные соглашения, принимает меры по выполнению международных договоров РФ о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;
- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства РФ;

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;
- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;
- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства РФ о государственной тайне;
- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;
- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;
- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

Допуск должностных лиц и граждан к государственной тайне Допуск к государственной тайне – процедура оформления права

граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

Принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

- согласие на частные, временные ограничения их прав в соответствии со статьей 24 Закона «О государственной тайне»;
- письменное согласие на проведение в отношении их полномочий органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом «О государственной тайне»;
- ознакомление с нормами законодательства РФ о государственной тайне,

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

предусматривающими ответственность за его нарушение;

- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и/или штатных мероприятий.

Основанием для отказа гражданину в допуске к государственной тайне в соответствии со статьей 22 Закона «О государственной тайне» могут являться:

- признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения РФ;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное место жительства в другое государство;
- выявление в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;
- уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

- **первая форма** – для граждан, допускаемых к сведениям особой важности;
- **вторая форма** – для граждан, допускаемых к совершенно секретным сведениям;
- **третья форма** – для граждан, допускаемых к секретным сведениям. Наличие у должностных лиц и граждан допуска к сведениям более

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности РФ и ее территориальными органами.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом

Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

Основными **целями** контроля и надзора являются:

- обеспечение выполнения единых правил и норм в организации работ по защите государственной тайны;
- своевременное выявление предпосылок к утечке информации, составляющей государственную тайну.

Основными **задачами** контроля и надзора являются:

- оценка полноты и качества выполнения органами, организациями и должностными лицами, осуществляющими деятельность в области защиты государственной тайны, возложенных на них обязанностей и функций;
- оценка целесообразности и обоснованности принимаемых управленческих решений и мер по защите государственной тайны с целью предупреждения возможных неблагоприятных последствий их выполнения;
- выявление нарушений установленных требований или норм по защите государственной тайны, установление их причин, подготовка в необходимых случаях материалов для привлечения виновных к ответственности;
- профилактика различных видов нарушений;
- выявление нерешенных проблем и противоречий в правовом, организационном, научно-техническом, информационном и других видах обеспечения эффективной защиты государственной тайны.

Рассмотрим основные термины в области контроля и надзора за обеспечением защиты государственной тайны.

Контроль состояния защиты государственной службы – проверка соответствия организации и эффективности защиты информации, составляющей государственную тайну, установленным требованиям и/или нормам по защите государственной тайны.

Контроль организации защиты информации – проверка соответствия организации, наличия и содержания документов требованиям правовых,

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

организационно-распорядительных и нормативных документов в области защиты информации.

Контроль эффективности защиты информации – проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации.

Надзор – наблюдение, разновидность контроля, одна из форм деятельности различных государственных органов по обеспечению законности. Надзор – это контроль в форме правового регулирования. Эта форма применяется, прежде всего, для осуществления контроля за соблюдением законов, установленных норм, требований, стандартов. Органы надзора вправе при соответствующих обстоятельствах применять к объектам надзора меры административного принуждения. Необходимым условием надзора является отсутствие между субъектами и объектами надзора организационной соподчиненности.

Контрольные вопросы

Перечислите органы защиты государственной тайны.

1. Какие существуют методы защиты сведений, составляющих государственную тайну?
2. Перечислите органы защиты государственной тайны.
3. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.
4. Назовите цели и задачи контроля и надзора за обеспечением защиты государственной тайны.
5. Поясните сущность ведомственного контроля над обеспечением защиты государственной тайны.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9-10.

Правовое обеспечение защиты банковской, профессиональной и служебной тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Банковская тайна – защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов. К основным объектам банковской тайны относятся: тайна банковского счета, тайна операций по банковскому счету, тайна банковского вклада, тайна частной жизни клиента.

Банковская тайна является видом конфиденциальной информации или видом сведений, перечень которых достаточно четко определен законом.

Статья 857 «Гражданского кодекса РФ (Часть вторая)» от 26 января 1996 года № 14-ФЗ «Банковская тайна» содержит следующие нормы:

- 1) банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте;
- 2) сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям.

Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренном законом;

- 3) в случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Федеральный закон «О банках и банковской деятельности» от 2 декабря 1990 года № 395-1 содержит более расширенную группу норм (статья 26):

- Кредитная организация. Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

- Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям). Счетной палате Российской Федерации, органам государственной налоговой службы и налоговой полиции, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве.
- Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия прокурора – органами предварительного следствия по делам, находящимся в их производстве.
- Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям.
- Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.
- Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.
- За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

Таким образом, сведения, составляющие банковскую тайну, не устанавливаются по волеизъявлению субъекта предпринимательской деятельности – банка или иной кредитной организации, а это определенные законом сведения, которые принадлежат клиентам банка (банковский счет, банковский вклад, операции по счету, сведения о клиенте). При этом обязанность сохранять эти сведения является односторонней обязанностью

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

банка – клиент не связан этими обязательствами. Вторым отличием банковской тайны, выводящим ее за пределы частного случая коммерческой тайны, является тот факт, что банковская тайна может выступать как охранительный институт для личной и семейной тайны, если граждане желают сохранять в тайне свое финансовое положение.

Пользование информацией, составляющей профессиональную тайну

В сфере ГМУ широко распространена **профессиональная тайна**, которая представляет собой одну из самых специфических систем ограничений на доступ к информации. Профессиональная тайна чаще всего имеет дело с информационными блоками, защита от несанкционированного распространения которых является обязанностью субъекта в силу выполняемых им профессиональных функций. При этом в качестве субъекта, на который возлагается обязанность сохранения профессиональной тайны, может выступать как физическое, так и юридическое лицо. Соблюдение тайн представителями определенных профессий является их обязанностью, возникающей вне зависимости от того, урегулирована она какими-либо юридическими нормами либо нет. В этом случае обязательства по нераспространению сведений являются неотъемлемой частью самой профессии. Гражданин не обратился бы к адвокату, нотариусу или частнопрактикующему врачу, если бы не был уверен, что доверенные этому лицу сведения не будут сохранены в тайне от посторонних, которыми в данном случае являются любые третьи лица.

Система исходящих от государства норм поведения также не может оставаться в стороне от регулирования этой группы общественных отношений. Нормы законодательства, регулирующие данные отношения, характеризуются в целом двумя моментами:

- данные нормы содержатся в соответствующих профильных законах;
- как правило, эти нормы содержат только запреты на распространение определенных категорий сведений, не описывая механизма их защиты.

Объектом профессиональной тайны является, прежде всего, информация, принадлежащая гражданам, обращающимся за профессиональными услугами (нотариальными, страховыми, медицинскими и др.). С развитием рыночных отношений и появлением большого числа субъектов предпринимательской деятельности в России юридические лица также стали полноправными участниками этих отношений. Нотариальная тайна, тайна связи, адвокатская тайна – действие этих правовых институтов в равной степени распространяется и на сведения, обладателями которых являются юридические лица.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Профессиональная тайна является неотъемлемой частью определенных видов профессиональной деятельности вне зависимости от того, ведется она от имени государства или от частного лица. И даже если она ведется от имени государства, это не значит, что государство в лице других органов ГМУ может без ограничений получать доступ к таким сведениям.

К примеру, по действующему законодательству РФ информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при обследовании и лечении, составляют **врачебную (медицинскую) тайну**.

Включаемый в данный институт перечень сведений достаточно подробно представлен в действующем законодательстве РФ. Прежде всего следует отметить нормы статьи 61 «Основ законодательства РФ об охране здоровья граждан», утвержденные ВС РФ 22 июля 1993 года № 5487-1, которая именуется «Врачебная тайна». На основе этих норм к медицинской тайне относятся:

- факт обращения гражданина за медицинской помощью;
- состояние здоровья гражданина;
- диагноз заболевания;
- иные сведения, полученные при обследовании и лечении.

Допускается предоставление сведений, составляющих медицинскую тайну, без согласия гражданина или его законного представителя:

- в целях обследования гражданина, не способного выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством;
- в случае оказания помощи несовершеннолетнему в возрасте до 15 лет для информирования его родителей или законных представителей;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий.

Нотариальная тайна вытекает из законодательной базы деятельности нотариата в РФ, которую определяет Конституция РФ и Основы законодательства РФ о нотариате.

Адвокатская тайна – сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи.

Процессуальные тайны – тайна совещания судей, тайна совещания присяжных заседателей, данные предварительного следствия (дознания) –

содержат в себе признаки как служебной тайны, так и профессиональной.

Первые два вида направлены на обеспечение невмешательства в отправление правосудия и представляют из себя административно-правовой запрет на контакт с судьями в период их совещания по поводу вынесения приговора (вердикта, решения).

Тайна страхования – это разновидность служебной, а также коммерческой тайны. Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о застрахованном лице, о состоянии его здоровья, а также о его имущественном положении.

Тайна связи – регулируется конституционными нормами (часть 2 статьи 23 Конституции РФ), а также соответствующими нормами федеральных законов «О связи» от 07 июля 2003 года № 126-ФЗ, «О почтовой связи» от 17 июля 1999 года № 176-ФЗ.

Пользование информацией, составляющей служебную тайну

В сфере ГМУ нередко фигурирует служебная тайна, которая наиболее сложна с точки зрения определения ее понятия и правового режима, поскольку в этот вид тайны в разное время включалось и теперь включается различное содержание. Служебная тайна является разновидностью конфиденциальной информации. Согласно Закону РФ «О государственной тайне» от 21 июля 1993 года № 5485-1, прежний режим служебной тайны упразднен, и секретные сведения относятся к государственной тайне. Однако в различных правовых актах термин «служебная тайна» продолжает упоминаться и в него вкладывается различное значение, причем в большинстве случаев оно даже не раскрывается.

Объектами служебной тайны являются преднамеренно скрываемые интересы и сведения о различных сторонах и сферах государственной, военной, управленческой, научно-технической, финансовой, экономической и др. деятельности хозяйствующего субъекта, охрана которых обусловлена возможной угрозой безопасности хозяйствующего субъекта.

Субъектами служебной тайны являются собственник служебной информации ограниченного распространения (юридическое лицо, обладающее на законном основании служебной конфиденциальной информацией), конфиденент служебной информации ограниченного распространения (физическое или юридическое лицо, использующее служебную информацию ограниченного распространения в пределах, установленных собственником или владельцем служебной информации ограниченного распространения на основании договора или распорядительных документов).

Содержащие служебную тайну документы:

- печатаются в специально выделенной комнате;

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

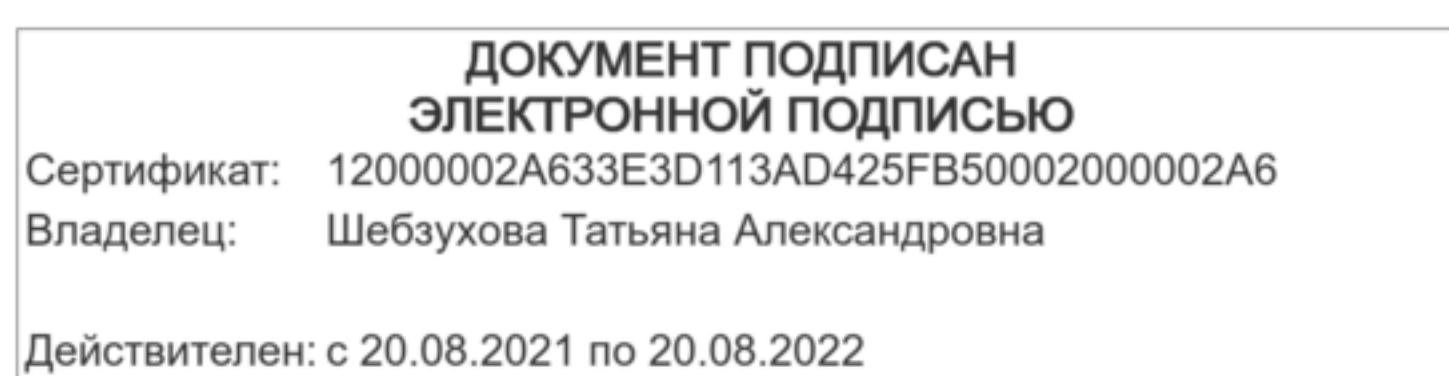
- учитываются, как правило, отдельно от несекретной документации;
- передаются работникам подразделений под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются только с письменного разрешения соответствующего руководителя;

Контрольные вопросы

1. Какие сведения относятся к банковской тайне?
2. Перечислите известные вам виды профессиональной тайны.
3. Раскройте порядок обращения с документами, содержащими служебную тайну.
4. Какая информация относится к сведениям конфиденциального характера?
5. Какие сведения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещено относить к конфиденциальной информации?
6. Опишите структуру законодательства РФ о коммерческой тайне.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.



ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 11-12

Правовое обеспечение защиты коммерческой тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Конфиденциальная информация – достаточно широкое понятие, поскольку к этой категории (за исключением сведений, относящихся к государственной тайне) относятся все виды информации ограниченного доступа, защищаемой законами. В соответствии с Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188 к этим сведениям относятся:

- 1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- 2) сведения, составляющие тайну следствия и судопроизводства;
- 3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
- 4) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);
- 5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);
- 6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Расширительному толкованию этот перечень не подлежит. Поэтому

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

произвольное отнесение кем-либо к разряду конфиденциальной другой, не предусмотренной перечнем информации не влечет за собой правовых последствий. Более того, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ запрещено относить к конфиденциальной информации:

- 1) законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- 2) документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- 3) документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
- 4) документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений и организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК.

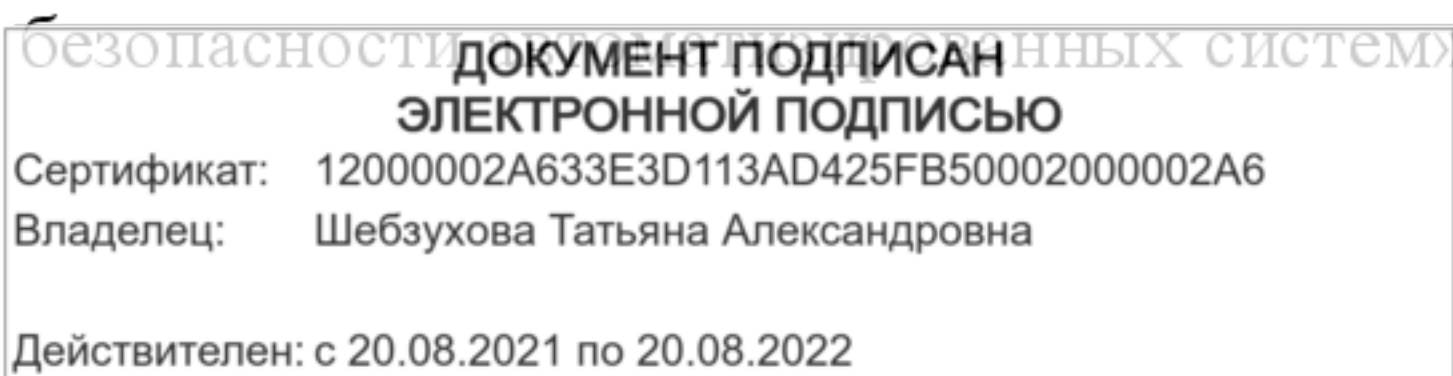
Под технической защитой конфиденциальной информации

понимается комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

В соответствии с Положением «О лицензировании деятельности по технической защите конфиденциальной информации» лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

- 1) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности

«компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность



телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

- 2) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами РФ, руководящими и нормативно-методическими документами, утвержденными приказами ФСТЭК, которые зарегистрированы в Министерстве юстиции РФ;
- 3) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;
- 4) использование третьими лицами программ для ЭВМ или баз данных на основании договора с их правообладателем.

Законодательство Российской Федерации о коммерческой тайне

В условиях рыночного хозяйствования коммерческая тайна защищает производителя от недобросовестной конкуренции, к которой относятся противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т. п.

Законодательство Российской Федерации о коммерческой тайне есть совокупность федеральных законодательных актов, которые содержат правовые нормы, регулирующие группу однородных общественных отношений, возникающих в связи и по поводу коммерческой тайны между ее обладателем и иными субъектами.

Закон «О предприятиях и предпринимательской деятельности» от 25 декабря 1990 года № 445-1 впервые закрепил понятие «коммерческая тайна»: информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Федеральный закон «О коммерческой тайне»

Федеральный закон «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

Положения закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована и не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

законодательства Российской Федерации о государственной тайне.

Основные понятия и определения

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну (секрет производства) – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Предоставление информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информация, относящаяся к коммерческой тайне

Состав сведений, составляющих коммерческую тайну, представляет собой одно из центральных звеньев в системе мер, осуществляемых предприятием по защите своей интеллектуальной собственности. Ошибочное или несвоевременное выделение предмета защиты существенно снижает эффективность системы информационной безопасности предприятия, что чревато существенным экономическим ущербом для него.

Перечень сведений, составляющих коммерческую тайну предприятия, следует формировать по следующим признакам:

- эта информация должна быть экономически выгодной для предприятия или выгодной для его конкурента в случае ее утечки. В качестве критерия важности конкретной информации принимается количественный показатель величины наносимого ущерба;
- эта информация не должна быть общеизвестной или общедоступной на законных основаниях;
- эти сведения не должны содержать государственной тайны или защищаться согласно нормам авторского или патентного права;
- информация, которая зафиксирована в письменной или иной материальной форме или находится в исключительном ведении предприятия;
- такая информация должна быть понятным образом специально обозначена («грифована») и в отношении нее должны быть обеспечены необходимые меры по сохранению конфиденциальности;
- эти сведения не должны напрямую касаться деятельности предприятия, способной нанести ущерб обществу, жизни и здоровью людей.

При этом информация, подтверждающая сведения, компрометирующие компанию, не может быть только на этом основании отнесена к коммерческой тайне.

Обеспечение конфиденциальности требует определенных затрат, в число которых входят, с одной стороны, затраты на обеспечение режимных мероприятий, а с другой – потери от ограничений в использовании

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

конфиденциальной информации. Экономический же эффект от утаивания информации может выразиться как в получении реальной прибыли, так и в предотвращении возможного ущерба предприятию. Сравнение положительных и отрицательных последствий ограничения доступа к рассматриваемым сведениям и их открытого использования, анализ возможностей предприятия по обеспечению необходимых защитных мер позволит определить экономическую или иную целесообразность отнесения тех или иных сведений к коммерческой тайне.

С течением времени ценность информации уменьшается, а суммарные затраты растут. Чем выше уровень защиты, тем дороже обходится ее обеспечение, поэтому необходимо оценивать оптимальный уровень защиты.

Самое сложное из приведенных понятий – отсутствие доступа на законном основании. За этой формулировкой стоят перечни сведений, которые запрещено относить к тому или иному виду тайны.

В законе «О коммерческой тайне» приведены сведения, которые не могут составлять коммерческую тайну.

Таким образом, режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

В статье 10 закона «О коммерческой тайне» приведены меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, или лиц, которым такая информация была предоставлена или передана;
- 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- 5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, приведенных выше.

Наряду с приведенными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Кроме того, меры по охране конфиденциальности информации признаются разумно достаточными, если:

- 1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- 2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Контрольные вопросы

1. Что представляет собой информация, составляющая коммерческую тайну?
2. Что понимается под разглашением информации, составляющей коммерческую тайну?
3. По каким признакам определяется перечень сведений, составляющих коммерческую тайну предприятия?
4. В отношении каких сведений не может быть установлен режим коммерческой тайны?
5. Приведите меры по охране конфиденциальности информации в соответствии с законом «О коммерческой тайне».

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 13-14

Правовое обеспечение защиты персональных данных

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

По смыслу Конституции РФ **личность** – это человек как член общества и как носитель индивидуального начала. Главное в конституционном понятии личности – это социальная ценность человека, в соответствии с чем он является субъектом различных прав, свобод и обязанностей.

Сущность информационной свободы состоит, по крайней мере, из четырех правомочий: право на индивидуализацию; право на защиту чести и достоинства; право на дачу согласия на сбор, хранение и использование материалов о частной жизни; право на неприкосновенность частной жизни, личную и семейную тайну.

Право на неприкосновенность частной жизни, личную и семейную тайну означает, что человек вправе строить свою жизнь в семье, в неформальном общении с друзьями и другими лицами таким образом, как он сам того желает.

В Российском законодательстве существуют следующие источники права на личную или семейную тайну:

1. Конституция РФ признает права и свободы человека высшей ценностью, а их защиту – обязанностью государства.
2. Федеральный Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ регулирует отношения, возникающие при:
 - формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
 - создании и использовании информационных технологий и средств их обеспечения;
 - защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

3. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ регулирует отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

4. Уголовный кодекс РФ. Статья 137. Нарушение неприкосновенности частной жизни.

Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

4. Трудовой кодекс РФ. Осуществляет защиту персональных данных работника – информации, необходимой работодателю в связи с трудовыми отношениями.

5. Гражданский кодекс РФ. Статьи 150-152, призванные защитить право человека на неприкосновенность частной жизни.

Наиболее емким потоком конфиденциальной информации являются сведения о гражданах. Действующее законодательство определяет их как персональные данные. Это понятие было введено Федеральным Законом «Об информации, информатизации и о защите информации» и получило дальнейшее развитие в Указе Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188.

Предметом личной и семейной тайны являются следующие сведения:

1. О фактах биографии.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

2. О состоянии здоровья человека.
3. Об имущественном положении.
4. О роде занятий и совершенных поступках.
5. О взглядах, оценках, убеждениях человека.
6. Об отношениях в семье, а также отношениях человека с другими людьми.

В соответствии с Федеральным законом «О персональных данных» под **персональными данными** понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных – действия, в результате которых

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

К персональным данным относятся: биографические и опознавательные данные, личные характеристики, сведения о семейном положении, социальном положении, образовании, навыках, профессии, служебном положении, финансовом положении, состоянии здоровья и прочее.

Обработка персональных данных должна осуществляться на основе принципов:

- 1) законности целей и способов обработки персональных данных и добросовестности;
- 2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- 3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 4) достоверности персональных данных, их достаточности для целей

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

- 5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении

целей обработки или в случае утраты необходимости в их достижении.

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных за исключением следующих случаев:

- 1) если обработка персональных данных осуществляется на основании Федерального закона «О персональных данных», устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- 2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- 3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- 4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- 5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- 6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- 7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев обезличивания персональных данных и в отношении

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

общедоступных персональных данных.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Независимо от вида деятельности на любом предприятии имеется информация, требующая защиты. На коммерческом предприятии это коммерческая тайна и персональные данные сотрудников (ПДР).

Персональные данные работника – информация о конкретном лице, необходимая работодателю в связи с возникновением трудовых отношений.

Данная информация в соответствии с законодательством (Закон РФ «Об информации, информационных технологиях и о защите информации») является конфиденциальной. На каждого работника ведется личное дело, в состав которого входят данные, представленные на рисунке 2.3.

Согласно «Перечню типовых управленческих документов, образующихся в деятельности организаций с указанием сроков хранения», личные дела рядовых работников предприятия должны храниться 75 лет, а руководителей – постоянно.

Личные дела работников хранятся как документы, доступ к которым ограничен.

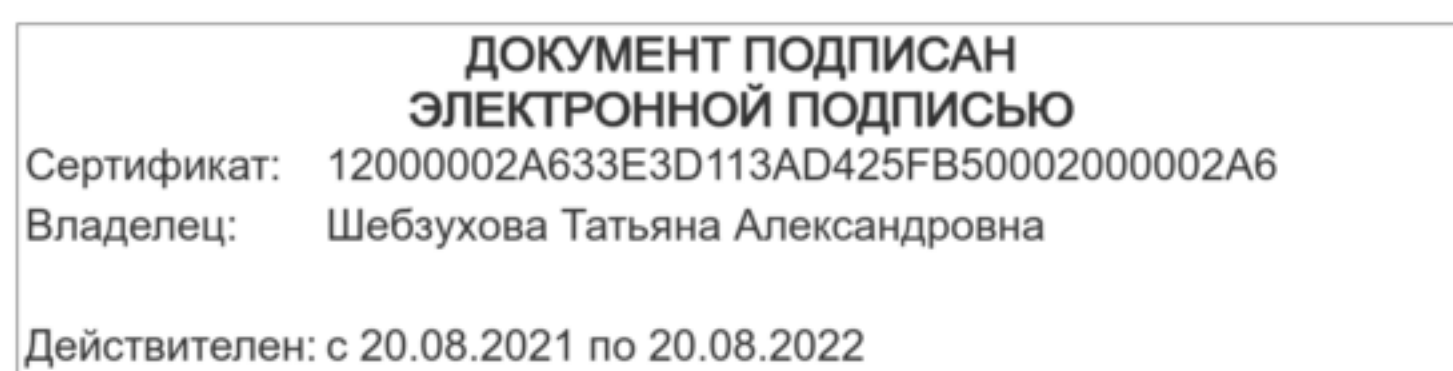
Отбор документов предприятия на хранение или уничтожение осуществляется по решению экспертной комиссии, руководствующейся федеральными, отраслевыми и внутренними нормативными актами, например:

- «Положение об Архивном фонде РФ»;
- «Основные правила работы ведомственных архивов»;
- «Положение об экспертной комиссии»;
- «Номенклатура дел»;
- «Инструкция по делопроизводству» и др.

Экспертиза ценности документов производится ежегодно. Документы по личному составу или содержащие КТ, отобранные на хранение, требуют дополнительного оформления:

- производится нумерация листов в правом верхнем углу;
- составляется внутренняя опись;
- дело переплетается и прошивается в четыре прокола. Опись дел по личному составу обозначают: опись №1 л/с.

Очень важной и дорогостоящей информацией фирмы являются сведения о



клиентах и конкурентах. Западные специалисты рекомендуют использовать два документа: «профиль клиента» и «профиль конкурента», которые должны постоянно пополняться и обновляться информацией. Эти базы данных позволяют найти индивидуальный подход к деловому партнеру и предвидеть шаги конкурентов.

Доказательством высокого качества делового партнерства и обеспечения интересов клиента служит наличие на фирме сертификата по Международной системе стандартов качества ISO 9000. В настоящее время система ISO оценивает не только качество конечного продукта бизнеса, но и сам бизнес- процесс предприятия: проектирование, разработку, закупку сырья и комплектующих, создание, обработку, документирование, заключение контрактов, обучение персонала, обслуживание и поддержку клиентов и информационную безопасность.

По имеющимся данным к 2002 году 76 стран мира проводят сертификацию на соответствие стандартам ISO 9000. Сертификат получили более 100000 компаний. Наличие сертификата позволяет заключать сделки с ведущими мировыми компаниями, получать госзаказы, принимать участие в международных проектах. Исследования поведения компаний при проведении такой сертификации позволяет заглянуть под маску рекламного имиджа, что значительно увеличивает безопасность деловых отношений.

Неоправданный риск сомнительных сделок может серьезно отразиться на жизнеспособности предприятия. Результатом недобросовестной конкуренции может стать уничтожение или потеря значительной части информационных ресурсов предприятия. В ряде случаев такие потери могут привести к банкротству и ликвидации предприятия.

В Российской Федерации принят закон «О несостоятельности (банкротстве)» от 26 октября 2002 года № 127-ФЗ, определяющий условия банкротства и регламент действий и процедур в отношении должника.

Ответственность за нарушение норм защиты персональных данных

В соответствии с Трудовым кодексом РФ работодатель обязан соблюдать следующие требования при работе с персональными данными.

В соответствии со статьей 13.11 КоАП нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

В УК РФ уголовная ответственность в отношении ПДР дана в ст. 137

«Нарушение неприкосновенности частной жизни»: штраф в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

То же преступление, совершенное лицом с использованием своего служебного положения, наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

Контрольные вопросы

1. Назовите основные источники права в области защиты персональных данных.
2. Какие сведения являются предметом личной и семейной тайны?
3. Что понимается под обработкой персональных данных?
4. Поясните понятие «трансграничная передача персональных данных».
5. Перечислите принципы обработки персональных данных.
6. Какие требования необходимо выполнить при работе с персональными данными работника?

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 15-16

Правовое обеспечение защиты интеллектуальной собственности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Понятие интеллектуальной собственности (ИС) используется с момента создания 14 июля 1967 года Всемирной организации интеллектуальной собственности (ВОИС), но в советском законодательстве этот термин появился впервые в Законе СССР «О собственности в СССР»

(6 марта 1990 года), а в российском был утвержден в декабре 1993 года – с принятием Конституции РФ и с принятием первой части Гражданского кодекса РФ.

Наряду с упоминанием в ГК РФ был принят ряд законов:

- «Патентный закон Российской Федерации» от 23 сентября 1992 года № 3517-1;
- «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 23 сентября 1992 года № 3520-1;
- «О правовой охране топологий интегральных микросхем» от 23 сентября 1992 № 3526-1;
- «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 № 3523-1;
- «Об авторском праве и смежных правах» от 9 июля 1993 года № 5351-1.

К настоящему времени в Российской Федерации в отношении ИС действует четвертая часть Гражданского кодекса РФ от 18 декабря 2006 г., вступившего в силу с 1 января 2008 г. В Федеральном законе «О введении в действие части четвертой Гражданского кодекса Российской Федерации» от 18 декабря 2006 г. в ст. 2 приведен перечень нормативно-правовых актов, утративших силу с 1 января 2008 г., среди которых были и перечисленные

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

выше законы. Нормы Гражданского кодекса РФ (в дальнейшем – ГК) образуют в своей совокупности особую подотрасль российского гражданского права – право интеллектуальной собственности. С учетом общности ряда объектов интеллектуальной собственности указанная подотрасль российского гражданского права обычно подразделяется на четыре относительно самостоятельных института. Несмотря на тесную взаимосвязь и наличие целого ряда общих моментов, каждый из этих институтов имеет присущие лишь ему черты, которые находят отражение в нормах российского законодательства.

Прежде всего выделяется *институт авторского права и прав, смежных с авторским*. Им регулируются отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного и кабельного вещания (смежные права). Объединение в едином институте, который в дальнейшем для краткости будет именоваться авторским правом, двух указанных групп норм объясняется теснейшей зависимостью возникновения и осуществления смежных прав от прав авторов творческих произведений, а также регулирование соответствующих отношений единым законом.

Другим правовым институтом, входящим в систему подотрасли «право интеллектуальной собственности», является *патентное право*. Оно регулирует имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием и использованием изобретений, полезных моделей и промышленных образцов.

С развитием товарно-денежных отношений в России все более важным элементом рыночной экономики становятся такие объекты промышленной собственности, как фирменные наименования, товарные знаки, знаки обслуживания и наименования мест происхождения товаров. Создание равных условий хозяйствования для всех товаровладельцев, внедрение конкурентных начал в их деятельность и повышение ответственности за ее результаты, необходимость насыщения рынка товарами и услугами для удовлетворения потребностей населения обуславливают объективную потребность в правовом механизме, обеспечивающем должную индивидуализацию предприятий и организаций, а также производимых ими товаров и услуг. Такой правовой механизм представлен особым институтом рассматриваемой подотрасли гражданского права, а именно *институтом средств индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг)*. Данный правовой институт, как и патентное право, имеет дело с так называемой промышленной собственностью, то есть с исключительными правами, реализуемыми в сфере производства, торгового обращения, оказания

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

услуг и т. п. Основной функцией рассматриваемого института интеллектуальной собственности является обеспечение должной индивидуализации производителей и их товаров, работ и услуг.

Творения, признаваемые произведениями науки, литературы или искусства, а также изобретениями, полезными моделями и промышленными образцами, не исчерпывают всего многообразия результатов творческой деятельности. Наряду с ними имеется немало объектов, которые создаются творческими усилиями людей, представляют ценность для общества и также нуждаются в общественном признании и правовой охране. Помимо традиционных объектов, охраняемых авторским и патентным правом, а также институтом средств индивидуализации участников гражданского оборота, российское гражданское право предоставляет охрану селекционным достижениям, топологиям интегральных микросхем, информации, составляющей служебную и коммерческую тайну, и некоторым другим результатам интеллектуальной деятельности. Опираясь на отличия указанных результатов интеллектуальной деятельности от традиционных объектов интеллектуальной собственности, все их можно условно отнести к сфере единого правового института, а именно *института охраны нетрадиционных объектов интеллектуальной собственности*.

Современное российское законодательство об ИС подразделяется на пять основных частей:

- авторское право;
- охрана смежных прав;
- патентное право;
- законодательство о средствах индивидуализации участников гражданского оборота, товаров и услуг;
- законодательство о нетрадиционных объектах ИС (научные открытия, рацпредложения, ноу-хау);
- законодательство о защите против недобросовестной конкуренции.

Каждый из этих институтов имеет свои особенности. Рассмотрим основные из них при краткой характеристике каждого по структуре: источники права; объекты и субъекты права; основные права субъектов; способы их охраны и защиты.

Результатом интеллектуальной деятельности человека является информационный продукт, который представляется на рынке в виде информационных товаров и услуг.

Свойство информационного продукта, такое как трудность производства и относительная простота тиражирования создает немало проблем в связи с определением прав собственности в области информационной деятельности.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

Законодательными актами РФ регламентируется право собственности на информацию, полученную юридическими и физическими лицами в результате интеллектуальной деятельности. Это исключительное право представляет собой интеллектуальную собственность (ИС).

Под **интеллектуальной собственностью** понимаются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.

Конкретизация понятия интеллектуальная собственность дана в Конвенции, учреждающей Всемирную организацию интеллектуальной собственности (ВОИС). Конвенция была принята на Стокгольмской конференции в 1967 году и ратифицирована в 1968 году СССР.

Правовая охрана интеллектуальной собственности

Существует три общепризнанные в мире правовые формы защиты интеллектуальной собственности: авторское право, патентное право и коммерческая тайна.

Авторское право – форма правовой защиты в отношении литературных, художественных и научных произведений.

Смежные права – это права, примыкающие к авторскому праву, они защищают: исполнителей (актеров, певцов, танцоров и т. д.); производителей фонограмм; организации эфирного и кабельного вещания.

Патентное право – форма правовой защиты в отношении изобретений во всех областях человеческой деятельности.

Коммерческая тайна – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам. К информации, составляющей КТ, относят сведения, которые называют «ноу-хау».

Ноу-хау – не являющиеся общеизвестными и практически применяемые в производственной и хозяйственной деятельности: различного рода технические знания и опыт, включая методы, способы и навыки; разработки и использования технологических процессов; методы и способы лечения и т. п.

Объекты патентного права

Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие установленным настоящим кодексом требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере художественного конструирования, отвечающие установленным ГК РФ требованиям к

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

промышленным образцам. На изобретения, содержащие сведения, составляющие государственную тайну (секретные изобретения), положения ГК РФ распространяются, если иное не предусмотрено специальными правилами статей 1401–1405 ГК РФ и изданными в соответствии с ними иными правовыми актами. Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана в соответствии с настоящим кодексом не предоставляется.

Не могут быть объектами патентных прав:

- 1) способы клонирования человека;
- 2) способы модификации генетической целостности клеток зародышевой линии человека;
- 3) использование человеческих эмбрионов в промышленных и коммерческих целях;
- 4) иные решения, противоречащие общественным интересам, принципам гуманности и морали.

В качестве **изобретения** охраняется техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств). Изобретению предоставляется правовая охрана, если оно является:

- новым – оно не известно из уровня техники
- имеет изобретательский уровень – если для специалиста оно не следует из уровня техники явным образом.
- промышленно применимо – если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

Уровень техники включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

При установлении новизны изобретения в уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патентов на изобретения и полезные модели, с документами которых вправе ознакомиться любое лицо и запатентованные в Российской Федерации изобретения и полезные модели.

Раскрытие информации, относящейся к изобретению, автором изобретения, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности изобретения стали общедоступными, не является обстоятельством, препятствующим

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

признанию патентоспособности изобретения, при условии, что заявка на выдачу патента на изобретение подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности изобретения, имели место, лежит на заявителе.

Не являются изобретениями:

- 1) открытия;
- 2) научные теории и математические методы;
- 3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;
- 4) правила и методы игр, интеллектуальной или хозяйственной деятельности;
- 5) программы для ЭВМ;
- 6) решения, заключающиеся только в представлении информации.

В соответствии с ГК РФ исключается возможность отнесения этих объектов к изобретениям только в случае, когда заявка на выдачу патента на изобретение касается этих объектов как таковых.

Не предоставляется правовая охрана в качестве изобретения:

- 1) сортам растений, породам животных и биологическим способам их получения, за исключением микробиологических способов и продуктов, полученных такими способами;
- 2) топологиям интегральных микросхем.

В качестве **полезной модели** охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если она является новой (если совокупность ее существенных признаков не известна из уровня техники) и промышленно применимой (если она может быть использована в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере).

Уровень техники включает опубликованные в мире сведения о средствах того же назначения, что и заявленная полезная модель, и сведения об их применении в Российской Федерации, если такие сведения стали общедоступными до даты приоритета полезной модели. В уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патента на изобретения и полезные модели, с документами которых вправе ознакомиться любое лицо в соответствии с пунктом 2 статьи 1385 или пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации изобретения

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

и полезные модели.

Раскрытие информации, относящейся к полезной модели, автором полезной модели, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности полезной модели стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности полезной модели, при условии, что заявка на выдачу патента на полезную модель подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности полезной модели, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве полезной модели:

- 1) решениям, касающимся только внешнего вида изделий и направленным на удовлетворение эстетических потребностей;
- 2) топологиям интегральных микросхем.

В качестве **промышленного образца** охраняется художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид.

Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным. К существенным признакам промышленного образца относятся признаки, определяющие эстетические и (или) эргономические особенности внешнего вида изделия, в частности, форма, конфигурация, орнамент и сочетание цветов.

Промышленный образец является новым, если совокупность его существенных признаков, нашедших отражение на изображениях изделия и приведенных в перечне существенных признаков промышленного образца (пункт 2 статьи 1377), не известна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца. При установлении новизны промышленного образца также учитываются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на промышленные образцы, с документами которых вправе ознакомиться любое лицо в соответствии с пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации промышленные образцы.

Промышленный образец является оригинальным, если его существенные признаки обусловлены творческим характером особенностей изделия.

Раскрытие информации, относящейся к промышленному образцу, автором промышленного образца, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

сущности промышленного образца стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности промышленного образца, при условии, что заявка на выдачу патента на промышленный образец подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности промышленного образца, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве промышленного образца:

- 1) решениям, обусловленным исключительно технической функцией изделия;
- 2) объектам архитектуры (кроме малых архитектурных форм), промышленным, гидротехническим и другим стационарным сооружениям;
- 3) объектам неустойчивой формы из жидких, газообразных, сыпучих или им подобных веществ.

Субъекты патентного права

К основным субъектам патентного права относятся авторы (изобретения, полезной модели, промышленного образца), патентообладатели, их правопреемники, патентное ведомство, патентные поверенные.

Автор – любое физическое лицо, творческим трудом которого созданы изобретение, полезная модель, промышленный образец, селекционное достижение.

За лиц до 14 лет права осуществляют их законные представители (родители, опекуны).

Не признаются авторами физические лица, не внесшие личного творческого вклада в создание объекта промышленной собственности, оказавшие автору только техническую, организационную или материальную помощь, либо только способствовавшие оформлению прав на его использование.

Патентообладатель – лицо, владеющее патентом на изобретение, промышленный образец, свидетельством на полезную модель, селекционное достижение и вытекающими из патента (свидетельства) исключительными правами на использование указанных объектов.

Патентообладателями могут быть:

- авторы изобретения, полезной модели, промышленного образца, селекционного достижения; их наследники или иные правопреемники;
- физические и юридические лица (при условии их согласия), указанные автором или его правопреемником в заявлении, поданном в Патентное ведомство

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

до момента регистрации изобретения, полезной модели, промышленного образца;

- работодатели – в отношении объектов промышленной собственности, созданных работником в связи с выполнением служебного задания, с выплатой последнему вознаграждения в размере и на условиях специального соглашения между ними.

Наследники – могут быть по закону и по завещанию. Если умерший патентообладатель не оставил завещания и не имел законных наследников, то в качестве наследника, в отличие от авторского права, выступает государство в лице Федерального фонда изобретений России.

Патентное ведомство – федеральный орган исполнительной власти, обеспечивающий формирование и осуществление единой государственной политики в области правовой охраны промышленной собственности.

На Патентное ведомство возложены также задачи приема и рассмотрения заявок на изобретения, полезные модели и промышленные образцы;

проведения экспертизы по заявкам; государственной регистрации; выдачи патентов; публикации официальных сведений; издания патентных правил и разъяснений по применению Патентного закона и др.

Патентные поверенные – граждане РФ, имеющие в соответствии с законом право на представительство физических и юридических лиц перед Роспатентом и организациями, входящими в единую патентную службу.

В качестве патентного поверенного может быть аттестован (проверка документов и квалификационный экзамен) и зарегистрирован в Роспатенте (на основании личного заявления) гражданин РФ, имеющий постоянное местожительство в РФ, высшее образование и не менее четырех лет практической работы в этой сфере. Полномочия поверенных на ведение дел подтверждаются доверенностью.

Порядок получения патента

Заявка на выдачу патента на изобретение, полезную модель или промышленный образец подается в федеральный орган исполнительной власти по интеллектуальной собственности лицом, обладающим правом на получение патента в соответствии с настоящим кодексом (заявителем).

Заявление о выдаче патента на изобретение, полезную модель или промышленный образец представляется на русском языке. Прочие документы заявки представляются на русском или другом языке. Если документы заявки представлены на другом языке, к заявке прилагается их перевод на русский язык.

Заявление о выдаче патента на изобретение, полезную модель или

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

промышленный образец подписывается заявителем, а в случае подачи заявки через патентного поверенного или иного представителя – заявителем или его представителем, подающим заявку.

Требования к документам заявки на выдачу патента на изобретение, полезную модель или промышленный образец устанавливаются на основании 4 части ГК РФ федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности.

К заявке на выдачу патента на изобретение, полезную модель или промышленный образец прилагается документ, подтверждающий уплату патентной пошлины в установленном размере, или документ, подтверждающий основания освобождения от уплаты патентной пошлины, либо уменьшения ее размера, либо отсрочки ее уплаты.

Заявка на выдачу патента на изобретение (заявка на изобретение) должна относиться к одному изобретению или к группе изобретений, связанных между собой настолько, что они образуют единый изобретательский замысел (требование единства изобретения).

Заявка на изобретение должна содержать:

- 1) заявление о выдаче патента с указанием автора изобретения и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;
- 2) описание изобретения, раскрывающее его с полнотой, достаточной для осуществления;
- 3) формулу изобретения, выражающую его сущность и полностью основанную на его описании;
- 4) чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
- 5) реферат.

Датой подачи заявки на изобретение считается дата поступления в федеральный орган исполнительной власти по интеллектуальной собственности заявки, содержащей заявление о выдаче патента, описание изобретения и чертежи, если в описании на них имеется ссылка, а если указанные документы представлены не одновременно, – дата поступления последнего из документов.

Правовая охрана патентных прав

Правовая охрана на объекты промышленной собственности начинается с даты поступления заявки в Патентное ведомство и подтверждается патентом на изобретение, промышленный образец или свидетельством на полезную модель.

Заявка на выдачу патента подается автором, работодателем или их правопреемником в Патентное ведомство и должна содержать в себе:

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

- заявление о выдаче патента;
- описание разработки;
- формулу изобретения, полезной модели;
- чертежи, необходимые для понимания сущности разработки;
- реферат;
- комплект фотографий, макет или рисунок об общем виде изделия. Заявитель имеет право внести исправления и уточнения в материалы заявки без изменения сущности разработки до принятия решения о выдаче

патента. Если изменения были внесены по инициативе заявителя в течение двух месяцев со дня подачи заявки, патентная пошлина за внесение изменений не взимается.

После проведения экспертизы заявки Патентное ведомство при положительном результате устанавливает приоритет разработки и принимает решение о выдаче патента, по истечении 18 месяцев с даты поступления заявки публикует сведения о заявке, публикует в официальном бюллетене сведения о выдаче патента, одновременно внося разработку в соответствующий

Государственный реестр, выдает патент лицу, на имя которого он испрашивался.

В патентном праве различают:

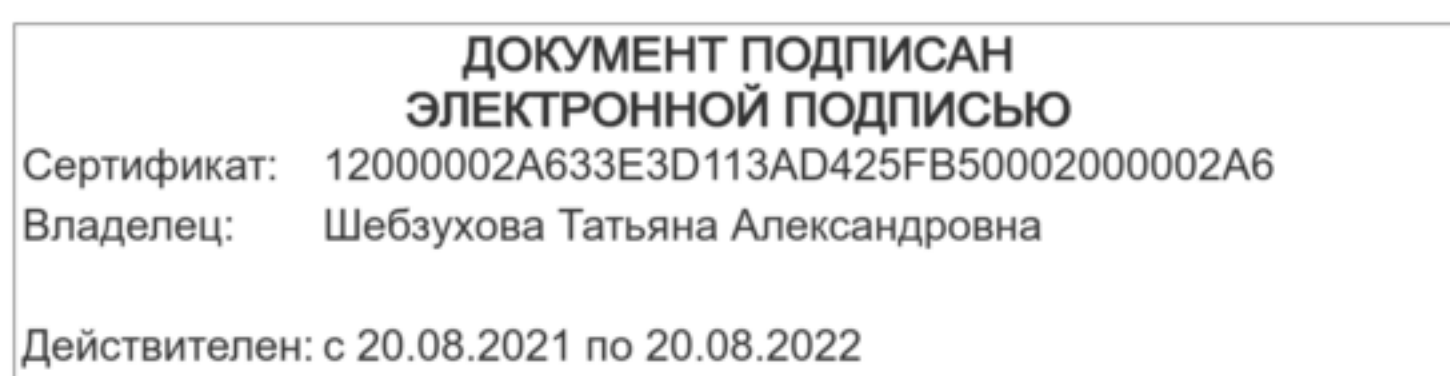
- 1) личные неимущественные права автора изобретения (право на авторство, право на имя, право на вознаграждение);
- 2) право на получение патента
- 3) исключительные (имущественные) права патентообладателя на использование разработок по своему усмотрению;
- 4) права патентообладателя по распоряжению патентом (уступка прав, выдача разрешения на использование запатентованных разработок).

Право авторства является неотчуждаемым личным правом и охраняется бессрочно. Имущественные (исключительные) права патентообладателя действуют с даты поступления заявки в Патентное ведомство в течение срока действия патента (на изобретение – 20 лет, на полезную модель – 10 лет, на промышленный образец – 15 лет) и могут быть продлены. За поддержание патента и его продление патентообладатель обязан платить пошлины.

При признании патента полностью недействительным, при неуплате в установленный срок пошлины либо на основании заявления патентообладателя, действие патента прекращается досрочно.

Правовая охрана в соответствии с Патентным законом не предоставляется секретным изобретениям, полезным моделям, промышленным образцам.

Порядок обращения с такими разработками регулируется специальным



законодательством.

Защита патентных прав

Так же, как и в авторском праве, различают две основные формы защиты:

1. Неюрисдикционная – самозащита гражданами и организациями своих прав. Применяется редко.
2. Юрисдикционная – деятельность уполномоченных государством органов по принудительной защите прав и законных интересов авторов и патентообладателей в общем судебном порядке (через суды) и административном порядке (через Апелляционную палату Патентного ведомства и Высшую патентную палату).

В судебном порядке рассматриваются следующие споры:

- об авторстве на изобретение, полезную модель, промышленный образец;
- об установлении патентообладателя;
- о нарушении исключительного права на использование охраняемого объекта промышленной собственности и других имущественных прав патентообладателя;
- о заключении и исполнении лицензионных договоров на использование охраняемого объекта промышленной собственности;
- о выплате вознаграждения автору работодателем;
- о выплате компенсаций, предусмотренных Патентным законом.

Обязанность доказывания факта нарушения патента возлагается на патентообладателя.

В судебном порядке различают гражданско-правовые и уголовно-правовые способы защиты прав и законных интересов патентообладателей.

К основным способам гражданско-правовой защиты прав авторов и патентных прав относятся права требовать возмещение убытков виновными нарушителями.

Основным средством уголовно-правовой защиты является жалоба потерпевшего. Уголовная ответственность может наступить лишь в случае причинения крупного ущерба при незаконном использовании изобретения, полезной модели или промышленного образца, разглашения до официальной публикации без согласия автора или заявителя их сущности, присвоения авторства или принуждения к соавторству, и наказывается штрафом либо лишением свободы на срок до двух лет.

Общие положения об авторских и смежных правах

Источники авторского права

Основным источником авторского права РФ является четвертая часть Гражданского кодекса РФ, а также подзаконные нормативные акты – постановления Правительства РФ, ведомственные нормативно-правовые акты,

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

судебная практика, международные договоры и соглашения: Бернская конференция (1971 г.) об охране литературных и художественных произведений, Всемирная конвенция (1952 г.) об авторском праве, Римская конвенция (1961 г.) об охране прав артистов-исполнителей, изготовителей фонограмм и вещательных организаций и др.

Объекты авторского права

Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения:

- литературные произведения;
- драматические и музыкально-драматические произведения, сценарные произведения;
- хореографические произведения и пантомимы;
- музыкальные произведения с текстом или без текста;
- аудиовизуальные произведения;
- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;
- произведения декоративно-прикладного и сценографического искусства;
- произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов;
- фотографические произведения и произведения, полученные способами, аналогичными фотографии;
- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;
- другие произведения.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

Кроме того, к объектам авторских прав относятся производные произведения, то есть произведения, представляющие собой переработку другого произведения, и составные произведения, то есть произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), в форме

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 ГК РФ.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования. Не являются объектами авторских прав:

- 1) официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;
- 2) государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобное), а также символы и знаки муниципальных образований;
- 3) произведения народного творчества (фольклор), не имеющие конкретных авторов;
- 4) сообщения о событиях и фактах, имеющие исключительно информационный характер (сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное).

Авторские права распространяются на часть произведения, на его название, на персонаж произведения, если по своему характеру они могут быть признаны самостоятельным результатом творческого труда автора.

Объектами смежных прав являются:

- 1) исполнения артистов-исполнителей и дирижеров, постановки режиссеров-постановщиков спектаклей (исполнения), если эти исполнения выражаются в форме, допускающей их воспроизведение и распространение с помощью технических средств;
- 2) фонограммы, то есть любые исключительно звуковые записи исполнений или иных звуков либо их отображений, за исключением звуковой записи, включенной в аудиовизуальное произведение;
- 3) сообщения передач организаций эфирного или кабельного вещания, в том числе передач, созданных самой организацией эфирного или кабельного вещания либо по ее заказу за счет ее средств другой организацией;
- 4) базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

5) произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние, в части охраны прав публикаторов таких произведений.

Для возникновения, осуществления и защиты смежных прав не требуется регистрация их объекта или соблюдение каких-либо иных формальностей.

Предоставление на территории Российской Федерации охраны объектам смежных прав в соответствии с международными договорами Российской Федерации осуществляется в отношении исполнений, фонограмм, сообщений передач организаций эфирного или кабельного вещания, не перешедших в общественное достояние в стране их происхождения вследствие истечения установленного в такой стране срока действия исключительного права на эти объекты и не перешедших в общественное достояние в Российской Федерации вследствие истечения предусмотренного настоящим кодексом срока действия исключительного права.

Субъекты авторского права

К субъектам авторского права относятся:

- авторы (в том числе соавторы);
- наследники и иные правопреемники;
- организации, управляющие имущественными правами авторов на коллективной основе.

Субъектами смежных прав являются исполнители, производители фонограмм, организации эфирного или кабельного вещания.

Автор – это любое физическое лицо, независимо от возраста, гражданства и состояния дееспособности, творческим трудом которого создано произведение. Если произведение (в том числе программа для ЭВМ, база данных, топология) создано совместным творческим трудом двух и более физических лиц, каждое из этих лиц признается автором (соавтором).

Наследниками по закону являются только граждане (согласно очередности), а наследниками по завещанию – физические и юридические лица. Если умерший автор не оставил завещания и не имел законных наследников, то его авторские права прекращаются.

Организации, управляющие имущественными правами авторов и обладателей смежных прав на коллективной основе, создаются непосредственно обладателями авторских и смежных прав, действуют на основании устава и выполняют три основных функции: предоставление лицензий пользователям на соответствующие способы использования авторских произведений и объектов смежных прав, сбор вознаграждения за их использование и распределение этого вознаграждения обладателям авторских и смежных прав.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

Правовая охрана прав автора и смежных прав

Авторское право на произведение возникает в силу факта его создания, для своего осуществления не требует регистрации произведения, иного специального оформления или соблюдения каких-либо формальностей и носит исключительный характер.

Автору в отношении его произведения принадлежат личные неимущественные права и имущественные (исключительные) права.

Личные неимущественные права принадлежат автору независимо от его имущественных прав, сохраняются за ним в случае уступки (передачи) исключительных прав на использование произведения и включают в себя следующие основные права:

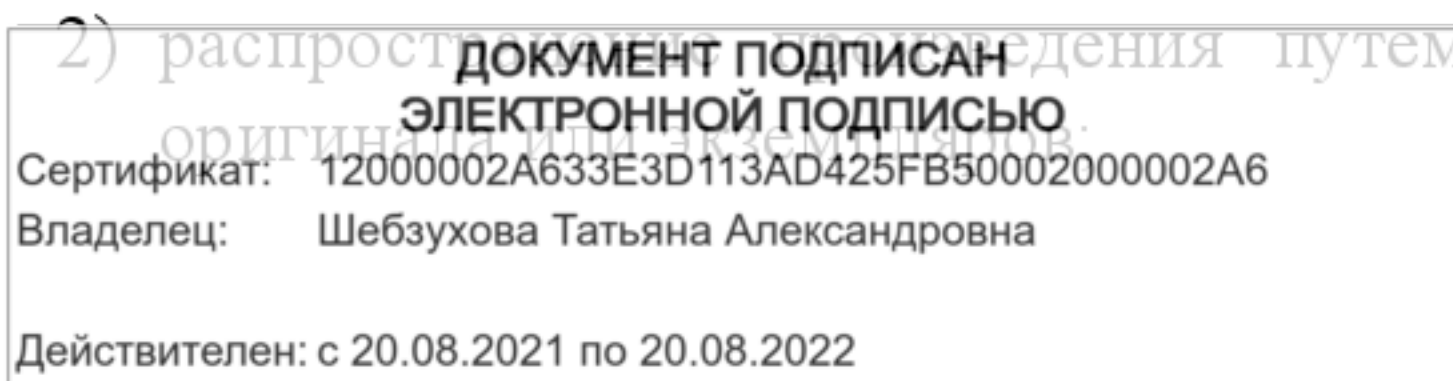
- 1) право авторства – право признаваться автором произведения;
- 2) право автора на имя – право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом или анонимно;
- 3) право на неприкосновенность произведения – не допускается без согласия автора внесение в его произведение изменений, сокращений и дополнений, снабжение произведения при его использовании иллюстрациями, предисловием, послесловием, комментариями или какими бы то ни было пояснениями;
- 4) право на обнародование – право обнародовать или разрешать обнародовать произведение в любой форме, включая право на отзыв. Право на отзыв реализуется с возмещением возможных убытков за счет автора.

Права на авторство, на имя, на защиту являются неотчуждаемыми и охраняются бессрочно.

Имущественные права – это исключительные права на использование произведений в любой форме и любым способом, которые включают в себя следующие права:

- 1) воспроизведение произведения, то есть изготовление одного и более экземпляра произведения или его части в любой материальной форме, в том числе в форме звуко- или видеозаписи, изготовление в трех измерениях одного и более экземпляра двумерного произведения и в двух измерениях одного и более экземпляра трехмерного произведения. При этом запись произведения на электронном носителе, в том числе запись в память ЭВМ, также считается воспроизведением, кроме случая, когда такая запись является временной и составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование записи или правомерное доведение произведения до всеобщего сведения;

- 2) распространение произведения путем продажи или иного отчуждения его



- 3) публичный показ произведения, то есть любая демонстрация оригинала или экземпляра произведения непосредственно либо на экране с помощью пленки, диапозитива, телевизионного кадра или иных технических средств, а также демонстрация отдельных кадров аудиовизуального произведения без соблюдения их последовательности непосредственно либо с помощью технических средств в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается произведение в месте его демонстрации или в другом месте одновременно с демонстрацией произведения;
- 4) импорт оригинала или экземпляров произведения в целях распространения;
- 5) прокат оригинала или экземпляра произведения;
- 6) публичное исполнение произведения, то есть представление произведения в живом исполнении или с помощью технических средств (радио, телевидения и иных технических средств), а также показ аудиовизуального произведения (с сопровождением или без сопровождения звуком) в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается произведение в месте его представления или показа либо в другом месте одновременно с представлением или показом произведения;
- 7) сообщение в эфир, то есть сообщение произведения для всеобщего сведения (включая показ или исполнение) по радио или телевидению (в том числе путем ретрансляции), за исключением сообщения по кабелю. При этом под сообщением понимается любое действие, посредством которого произведение становится доступным для слухового и (или) зрительного восприятия независимо от его фактического восприятия публикой. При сообщении произведений в эфир через спутник под сообщением в эфир понимается прием сигналов с наземной станции на спутник и передача сигналов со спутника, посредством которых произведение может быть доведено до всеобщего сведения независимо от его фактического приема публикой. Сообщение кодированных сигналов признается сообщением в эфир, если средства декодирования предоставляются неограниченному кругу лиц организацией эфирного вещания или с ее согласия;
- 8) сообщение по кабелю, то есть сообщение произведения для всеобщего сведения по радио или телевидению с помощью кабеля, провода, оптического волокна или аналогичных средств (в том числе путем ретрансляции). Сообщение кодированных сигналов признается сообщением по кабелю, если средства декодирования предоставляются неограниченному кругу лиц организацией

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

кабельного вещания или с ее согласия;

- 9) перевод или другая переработка произведения. При этом под переработкой произведения понимается создание производного произведения (обработки, экранизации, аранжировки, инсценировки и тому подобного). Под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя;
- 10) практическая реализация архитектурного, дизайнерского, градостроительного или садово-паркового проекта;
- 11) доведение произведения до всеобщего сведения таким образом, что любое лицо может получить доступ к произведению из любого места и в любое время по собственному выбору (доведение до всеобщего сведения).

Имущественные права автора могут быть ограничены случаями свободного использования:

1. Свободное воспроизведение произведения в личных целях. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях правомерно обнародованного произведения, за исключением:
 - воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений;
 - воспроизведения баз данных или их существенных частей;
 - воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса;
 - репродуцирования (пункт 2 статьи 1275) книг (полностью) и нотных текстов;
 - видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи;
 - воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.
2. Свободное использование произведения в информационных, научных, учебных или культурных целях. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

имени автора, произведение которого используется, и источника заимствования:

- цитирование в оригинале и в переводе в научных, полемических, критических или информационных целях правомерно обнародованных произведений в объеме, оправданном целью цитирования, включая воспроизведение отрывков из газетных и журнальных статей в форме обзоров печати;
- использование правомерно обнародованных произведений и отрывков из них в качестве иллюстраций в изданиях, радио- и телепередачах, звуко- и видеозаписях учебного характера в объеме, оправданном поставленной целью;
- воспроизведение в прессе, сообщение в эфир или по кабелю правомерно опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам или переданных в эфир произведений такого же характера в случаях, когда такое воспроизведение или сообщение не было специально запрещено автором или иным правообладателем;
- воспроизведение в прессе, сообщение в эфир или по кабелю публично произнесенных политических речей, обращений, докладов и других аналогичных произведений в объеме, оправданном информационной целью. При этом за авторами таких произведений сохраняется право на их опубликование в сборниках;
- воспроизведение или сообщение для всеобщего сведения в обзорах текущих событий средствами фотографии, кинематографии, путем сообщения в эфир или по кабелю произведений, которые становятся увиденными или услышанными в ходе таких событий, в объеме, оправданном информационной целью;
- воспроизведение без извлечения прибыли рельефно-точечным шрифтом или другими специальными способами для слепых правомерно опубликованных произведений, кроме произведений, специально созданных для воспроизведения такими способами.

В случае, когда библиотека предоставляет экземпляры произведений, правомерно введенные в гражданский оборот, во временное безвозмездное пользование, такое пользование допускается без согласия автора или иного правообладателя и без выплаты вознаграждения. При этом выраженные в цифровой форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, в том числе в порядке взаимного использования библиотечных ресурсов, могут предоставляться только в помещениях библиотек при условии исключения возможности создать копии этих произведений в цифровой форме.

Создание произведения в жанре литературной, музыкальной или иной пародии либо в жанре карикатуры на основе другого (оригинального)

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

правомерно обнародованного произведения и использование этой пародии либо карикатуры допускаются без согласия автора или иного обладателя исключительного права на оригинальное произведение и без выплаты ему вознаграждения.

3. Свободное использование произведения путем репродуцирования. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования репродуцирования в единственном экземпляре без извлечения прибыли:

- правомерно опубликованного произведения библиотеками и архивами для восстановления, замены утраченных или испорченных экземпляров произведения и для предоставления экземпляров произведения другим библиотекам, утратившим их по каким-либо причинам из своих фондов;
- отдельных статей и малообъемных произведений, правомерно опубликованных в сборниках, газетах и других периодических изданиях, коротких отрывков из правомерно опубликованных письменных произведений (с иллюстрациями или без иллюстраций) библиотеками и архивами по запросам граждан для использования в учебных или научных целях, а также образовательными учреждениями для аудиторных занятий.

Под репродуцированием (репрографическим воспроизведением) понимается факсимильное воспроизведение произведения с помощью любых технических средств, осуществляемое не в целях издания. Репродуцирование не включает воспроизведение произведения или хранение его копий в электронной (в том числе в цифровой), оптической или иной машиночитаемой форме, кроме случаев создания с помощью технических средств временных копий, предназначенных для осуществления репродуцирования.

4. Свободное использование произведения, постоянно находящегося в месте, открытом для свободного посещения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение, сообщение в эфир или по кабелю фотографического произведения, произведения архитектуры или произведения изобразительного искусства, которые постоянно находятся в месте, открытом для свободного посещения, за исключением случаев, когда изображение произведения таким способом является основным объектом этого воспроизведения, сообщения в эфир или по кабелю либо когда изображение произведения используется в коммерческих целях.

5. Свободное публичное исполнение музыкального произведения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения публичное исполнение музыкального произведения во время официальной или

в объеме, оправданном

религиозный документ, подписан	
ДОКУМЕНТ ПОДПИСАН	
ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

характером такой церемонии.

6. Свободное воспроизведение произведения для целей правоприменения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение произведения для осуществления производства по делу об административном правонарушении, для производства дознания, предварительного следствия или осуществления судопроизводства в объеме, оправданном этой целью.
7. Свободная запись произведения организацией эфирного вещания в целях краткосрочного пользования. Организация эфирного вещания вправе без согласия автора или иного правообладателя и без выплаты дополнительного вознаграждения делать запись в целях краткосрочного пользования того произведения, в отношении которого эта организация получила право на сообщение в эфир, при условии, что такая запись делается организацией эфирного вещания с помощью ее собственного оборудования и для собственных передач. При этом организация обязана уничтожить такую запись в течение шести месяцев со дня ее изготовления, если более продолжительный срок не согласован с правообладателем или не установлен законом. Такая запись может быть сохранена без согласия правообладателя в государственных или муниципальных архивах, если она носит исключительно документальный характер.
8. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ. Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:
 - внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программ или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;
 - изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные выше, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных предыдущим подпунктом.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;
- указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;
- информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

По общему правилу авторское право действует в течение всей жизни автора и 70 лет после его смерти, начиная с 1 января года, следующего после смерти.

Имущественные права передаются по договору. Имущественные права на использование служебного произведения принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное.

Правообладатель для оповещения о своих авторских правах на каждом экземпляре произведения вправе использовать знак охраны авторского права, состоящий из трех элементов: буквы «С» в окружности или в круглых скобках (С); имени правообладателя, года первого опубликования (выпуска в свет) произведения; для

оповещения о документальной базе на фонограмму – указывать

ДОКУМЕНТ ПОДПИСАН

ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

знак охраны в виде прописной буквы «Р», информации о самом правообладателе, года первого наименования фонограммы.

Исполнители (артисты, режиссеры, дирижеры) имеют как личные преимущественные, так и имущественные права при условии соблюдения ими прав автора исполняемого произведения, остальные объекты – только имущественные права.

Имущественные права обладателей смежных прав обеспечиваются их исключительным правом на использование исполнения, постановки, фонограммы, передачи в любой форме, в том числе право на вознаграждение за каждый вид использования исполнения, постановки, фонограммы, представления разрешения на использование передачи.

Защита авторских и смежных прав

Под защитой понимается совокупность мер, предусмотренных законом, по признанию, восстановлению прав и законных интересов их обладателей при нарушении или оспаривании этих прав и интересов.

Различают две основные формы защиты:

- 1) неюрисдикционная – самозащита гражданами и организациями своих прав и законных интересов в порядке необходимой обороны и крайней необходимости (отказ совершить определенные действия; отказ от исполнения договора в целом и т. п.). Применяется редко;
- 2) юрисдикционная – деятельность уполномоченных государством органов по принудительной защите прав и законных интересов их обладателей в судебном порядке или административном порядке.

Основным средством защиты в судебном порядке является иск, а в административном порядке – жалоба.

В судебном порядке различают по способам защиты прав и ответственности гражданско-правовые, административные и уголовно-правовые.

К основным способам гражданско-правовой защиты исключительных прав и законных интересов относится право требовать от нарушителя:

- признания прав;
- восстановления положения, существовавшего до нарушения права;
- прекращение действий, нарушающих право или создающих угрозу его нарушению (запрет на воспроизведение, на выпуск в свет, на распространение и т. п.);
- возмещение убытков;
- взыскания дохода, полученного нарушителем вследствие нарушения

пра

в;

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

- выплаты компенсации в определенных законом пределах;
- возмещения морального ущерба;
- прекращения или изменения договора в связи с действиями нарушителя;
- запрет совершать определенные действия ответчику (изготовление, воспроизведение, продажу, прокат и др.).

В случае наступления административной ответственности применяются:

- взыскание штрафа;
- обязательная конфискация по решению суда контрафактных (изготовленных или используемых с нарушением авторских прав) экземпляров произведений или фонограмм либо материалов и оборудования, используемых для их изготовления.

Контрольные вопросы

1. Перечислите основные законодательные акты, регламентирующие защиту интеллектуальной собственности.
2. Какие существуют институты защиты интеллектуальной собственности?
3. Перечислите и охарактеризуйте основные объекты интеллектуальной собственности.
4. Дайте определение понятиям «Изобретение», «полезная модель», «промышленный образец».
5. Назовите объекты патентного права.
6. Какие объекты патентного права не являются изобретениями?
7. Охарактеризуйте правовую основу защиты промышленного образца.
8. Перечислите и охарактеризуйте субъекты патентного права.
9. Перечислите объекты и субъекты авторского права.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 17-18.

Безопасность информационной инфраструктуры

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

Учебная и воспитательная цели:

Изучить понятие информационной инфраструктуры и теорию безопасности ее. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

- 1 Теория обеспечения безопасности информационной инфраструктуры

Краткие теоретические или справочно-информационные материалы

1 Теория обеспечения безопасности информационной инфраструктуры

Понятие «информация» — одно из базовых понятий теории обеспечения информационной безопасности. Объем явлений, охватываемых этим понятием, во многом определяет предмет обеспечения безопасности, характер угроз и методы противодействия этим угрозам.

В настоящее время отсутствует общепринятое представление о том, что такое информация. Однако критический анализ известных определений позволяет считать, что **информация** — это явление жизни организмов, заключающееся в отражении окружающей действительности для оценки происходящих в ней изменений и выбора системы действий по приспособлению

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

к этим изменениям.

Каждый тип организма обладает свойственной только ему совокупностью средств адаптации к изменениям окружающей действительности, что позволяет в определенных пределах обеспечивать приемлемые условия для протекания биохимических процессов, составляющих сущность организма. Уникальность средств адаптации каждого типа организмов обуславливает, в свою очередь, уникальность его «информационного» взгляда на мир, во многом не пересекающегося с «мировоззрением» других видов организмов.

По содержанию **информация** — это результат отображения в организме движения объектов окружающей действительности, включающей как материальную, так и нематериальную составляющие.

Известно, что материя в качестве субстанции выступает как объективная реальность, рассматриваемая со стороны ее внутреннего единства, безотносительно ко всем тем бесконечно многообразным видоизменениям, в которых она существует.

К числу самых важных категорий философии, обозначающих атрибуты материи, относят движение, отражение и взаимодействие.

Категория «движение» в материалистической философии определяет различные типы изменчивости, наблюдаемые в объективном мире начиная от перемещения объектов в пространстве и кончая процессами биологической и социальной эволюции. Категория «отражение» охватывает проявления свойства одних объектов материального мира воспроизводить в их природе особенности других взаимодействующих с ними объектов, т.е. свойства сохранять «следы» некоторых характеристик объектов взаимодействия. Наконец, категория «взаимодействие» описывает явления взаимного изменения объектов материального мира в процессе их движения.

Отражение взаимосвязано с взаимодействием и движением. Везде, где имеет место движение и взаимодействие, присутствует отражение.

В философии принято различать отражение в неживой и живой природе. В неживой природе отражение носит пассивный характер. Оно проявляется в виде

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

соответствующих изменений физических или химических свойств и состояний объектов, происходящих в результате внешнего воздействия. Отражение движения объектов материального мира в организмах, как было отмечено ранее, связано с изменением происходящих в них биохимических преобразований. Продукты измененных биохимических преобразований составляют материальную основу результата отражения движения в организмах, т.е. информации, а отраженный в организме образ действительности — его нематериальную основу. В мире взаимодействующих организмов информация проявляется в форме сведений и в форме сообщений.

Сведения представляют собой результат отражения окружающей действительности в организме.

Как уже было отмечено, каждый тип организмов обладает определенной, свойственной только ему «информационной» моделью мира. Эта модель возникает на основе обобщения сведений, отражаемых и накапливаемых организмом. Получаемые организмом сведения служат, с одной стороны, для формирования и актуализации «информационной» модели, выявления изменения состояния объектов материального мира, а с другой — для оценки возможных последствий выявленных изменений для существования организма и выбора рационального «варианта поведения». Структура «информационной» модели определяется генотипом организма. В наиболее простом виде данная модель включает отражаемые объекты реального мира, характеристики их состояния, оценки возможного влияния состояния этих объектов на жизнедеятельность организма, набор вариантов «поведения» организма в ситуациях, требующих реагирования, а также отношения (связи) между характеристиками состояния отражаемых объектов и вариантами «поведения».

Можно предположить, что «информационная» модель организмов, не обладающих большим разнообразием вариантов адаптации к изменениям окружающей действительности, имеет жесткую структуру, которая остается неизменной в течение их жизни. Структура «информационной» модели

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

организмов с достаточным разнообразием таких вариантов является гибкой, т.е. в определенных пределах может изменяться, накапливая сведения об окружающем мире.

Организмы, обладающие развитой нервной системой и психикой, имеют более широкие возможности как по модификации структуры «информационной» модели, так и по оперированию с содержащимися в ней сведениями. В частности, эти организмы способны вырабатывать **знания**, представляющие собой специфический вид сведений, отражающих закономерности изменения окружающей действительности и результативности использования имеющихся средств адаптации к данным изменениям. Специфика знаний заключается в том, что они являются результатом не непосредственного отражения движения каких-либо объектов действительности, а обобщения сведений о движениях этих объектов, накопленных в «информационной» модели. Знания позволяют организму прогнозировать на основе отражения реальной действительности позитивные и негативные последствия происходящих изменений или осуществляемых действий, что существенно повышает возможности его «комфортного» существования и выживания. Можно предположить, что способность выявления знаний появляется у организмов тогда, когда число возможных вариантов «поведения» становится значительным и их рефлекторное использование не позволяет обеспечить приемлемую эффективность адаптации.

Исключительно важную, с рассматриваемой точки зрения, часть живого мира образуют социальные организмы, условием существования которых является взаимодействие с другими такими же организмами. Их «информационные» модели, кроме сведений, получаемых самостоятельно, включают сведения, поступающие от других членов социума. Способность обмениваться сведениями реализуется через отправку и получение информации в форме сообщений.

Сообщение представляет собой набор знаков, с помощью которых сведения, накопленные одним организмом, могут быть переданы другому организму и восприняты им.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Способность обмениваться информацией реализуется организмами путем определенных алгоритмов кодирования сведений, т.е. Превращения их в набор знаков, воспринимаемых другими организмами и составляющих содержание сообщений, и алгоритмов декодирования поступающих сообщений, т.е. превращения набора знаков в сведения. При этом совершенно несущественно, каким именно способом осуществляется передача сообщения и какой набор знаков использован для его формирования.

Сведения, получаемые организмом от других организмов, образуют социальную составляющую его «информационной» модели мира, а совокупность этих составляющих «информационных» моделей взаимодействующих организмов — распределенную «информационную» модель социума, его «коллективный разум»- Одними из социальных организмов, существующих на Земле, являются человек и общество, которые обладают способностью отражать окружающую действительность в своей «информационной» модели мира в виде сведений, накапливать сведения, обобщать их и формировать знания, а также обмениваться сведениями с другими людьми и обществами.

С этой точки зрения информация представляет собой явление жизни и человека и общества, важнейший фактор их существования.

Информация в выделенных формах обладает во многом отличающимися свойствами, содержание которых отражено на рис. 2.

Приведенная трактовка сущности, содержания и форм информации не противоречит тому, как это понятие раскрывается и обыденной жизни и в праве. Так, в справочной литературе под информацией понимается «информирование о положении дел в какой-либо области, о каких-либо событиях; сообщение о положении дел где-либо, о каких-либо событиях; сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами». В федеральном законодательстве дефиниция «информация» раскрывается как «сведения (сообщения, данные) независимо от формы их представления»². Понятие «данные» можно рассматривать как разновидность

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

сообщений, предназначенных для автоматизированной обработки с использованием средств вычислительной техники. Эти сведения (сообщения, данные) могут отражать характеристики состояния объектов (лиц, предметов, фактов, событий) или движения конкретных объектов (явлений, процессов) окружающей действительности.

Не умаляя фундаментального характера теории информации, разработанной К.Шенноном, и методологического подхода к исследованию окружающей действительности, составляющего **основу** разработанной Н. Винером кибернетики, можно отметить, **что** используемая ими концепция

«информации» ограничивается рассмотрением только той составляющей этого явления, которая **имеет** форму сообщений. Применительно к ней раскрываются закономерности, связывающие количество двоичных знаков (**битов**), достаточных для описания одной буквы или знака **сообщения** (количество информации), с пропускной способностью **канала** связи, характеризуемой максимальным количеством **информации** (битов, достаточных для описания одного знака), которое **можно** передать по нему за одну секунду.

Таблица 2 - Формы информации и ее свойства

Формы информации	
Сведения – это результат отражения окружающей действительности в организме	Сообщения – это набор знаков, с помощью которого сведения, накопленные одним организмом, могут быть переданы другому организму и восприняты им
Свойства	
Духовность – это невозможность восприятия органами чувств	Материальность – способность воздействовать на органы чувств
Субъективность – зависимость количества и ценности сведений от получающего субъекта	Объективность – независимость от получающего их субъекта

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Неуничтожаемость невозможность физического уничтожения	—	Уничтожаемость — возможность физического уничтожения
Динамичность возможность изменения отношений между объектами материального мира, запечатленными в организме, и их характеристиками	—	Статичность — независимость набора знаков от времени, прошедшего с момента создания
Ограниченная воспроизводимость воспроизведения без закрепления на некотором носителе	—	невозможность точного

Вообще говоря, между количеством информации по К. Шеннону (т.е. количеством битов, достаточных для передачи одного **знака** сообщения) и количеством сведений (т.е. количеством **новых** элементов «информационной» модели человека, которые **возникают** вследствие осознания им сообщения) трудно установить **Какое** бы то ни было соотношение. Единственное, что можно в связи с этим отметить: если предположить, что каждый бит соответствует некоторому знаку, а знак, в свою очередь,

— элементу части передаваемой «информационной» модели, то количество информации по К.Шеннону позволяет оценить количество знаков, достаточных для кодирования этой части модели.

Теория информации К. Шеннона безусловно вскрыла ряд объективных закономерностей природы. В процессе развития этой теории последователями Шеннона произведено существенное расширение трактовки понятия «информация». «У большинства из тех, кто думал над этим кругом проблем, возникло предчувствие, что достаточно сделать небольшое обобщение, похожее на сделанное в свое время обобщение понятия энергии, и термин «информация» поможет установить какую-то глубинную закономерность нашего мира, эквивалентную по своему познавательному значению закону сохранения энергии». К сожалению, этого пока не произошло.

Другим выдающимся достижением, оказавшим существенное влияние на превращение понятия «информация» в общенаучную категорию, были разработанные Н.Винером основы кибернетики. Введенный им термин «кибернетика» был предназначен для обозначения всей теории управления и связи в машинах и живых организмах. В рамках этой работы Н.Винер также

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

пришел к понятию количества информации, но в результате изучения не проблем кодирования информации, а проблем сообщений и шумов в электрических фильтрах.

Наиболее известным научным результатом работы Н.Винера можно считать открытие достаточно широкого класса задач, связанных с поддержанием целенаправленного функционирования динамических объектов, а также метода «управления с помощью информирующей обратной связи», используемого в этих объектах. Существо этого метода в упрощенном виде может быть сформулировано как использование при управлении не только сведений о том, как должен двигаться управляемый объект, но и сведений о том, как он двигается к поставленной цели на самом деле. Для этого оцениваются отклонения параметров движения объекта от требуемых значений, на основе которых формируются управляющие воздействия на движущие элементы объекта в целях внесения требуемых изменений в это движение. Для реализации данного метода требуется наличие системы связи, передающей сообщения от управляющего центра к управляемым двигателям и обратно, что, естественно, требует исследования и собственно сообщений.

Объекты, в которых используется указанный метод управления, как правило, описываются линейными дифференциальными уравнениями, решения которых инвариантны к временным сдвигам. Широкая распространенность таких объектов в реальной жизни обусловила и большую востребованность кибернетических идей и методов при решении практических задач в различных сферах человеческой деятельности.

В то же время между управлением в технических системах и управлением в биологических и социальных системах наряду с наличием общих черт существуют и определенные различия. В биологических и социальных системах, как следует из вышеизложенного, управление осуществляется с использованием сведений, а в технических системах — с использованием сообщений. Вследствие этого управление в биологических и социальных системах не имеет той жесткости, которая свойственна управлению в технических системах. Если в

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

технической системе для оказания управляющего воздействия достаточно отправить сообщение или сигнал, то в биологических и социальных системах этого не всегда достаточно. Это особенно наглядно проявляется на примере социальных систем, в которых для реализации управляющего воздействия, как правило, требуется приложить определенные дополнительные усилия, чтобы индивиды, составляющие социальную систему, согласились выполнять такое управляющее воздействие.

Если в качестве управляемого объекта выступают отдельные органы человеческого организма, то управление практически не отличается от аналогичного процесса в технических системах. Это обусловлено особенностями человеческого организма, которые заключаются в том, что все его внутренние органы работают, как правило, независимо от сознания и с точки зрения управления образуют самостоятельные биологические системы со своей «информационной» моделью, слабо связанные с «информационной» моделью, используемой сознанием человека. Система управления такими органами и была выбрана Н.Винером в качестве объекта исследования. Если бы в качестве объекта исследования выступало сознание, то система управления выглядела бы значительно сложнее.

Передача сообщений через естественную среду обитания — воз-^{ДУХ} — обеспечивает обмен сведениями между индивидами, однако обладает рядом объективных ограничений по дальности и оперативности

осуществления информационного обмена, по длительности хранения переданных сообщений и возможности их ретроспективного анализа. Эти ограничения, в свою очередь, сказываются на активности

информационного взаимодействия между индивидами и, соответственно, на развитии социума, использовании имеющихся у него ресурсов и сил для адаптации к изменяющимся условиям существования.

Преодоление выделенного ограничения связано с созданием искусственной среды передачи информации, которая придаст процессу информационного взаимодействия новое качество. Способность организмов создавать такую искусственную среду существенно зависит от имеющихся у них

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

средств воздействия на окружающую действительность и от способности использовать коллективные действия для повышения эффективности адаптации. Наибольшими возможностями осуществления подобной деятельности обладает человек. Можно сказать, что если информация — явление жизни человека и общества, то **информационная инфраструктура** — это явление социальной жизни индивидов. Сущность данного явления заключается в разрешении противоречия между социально обусловленными потребностями в информационном обмене между членами общества для решения задач экономического, социального, политического и духовного развития и исторически обусловленными социальными и техническими возможностями удовлетворения этих потребностей.

Содержание данного явления общественной жизни определяется совокупностью используемых обществом информационных технологий и технических систем, реализующих эти технологии, а также совокупностью социальных институтов, обеспечивающих создание, эксплуатацию и модернизацию технических систем обеспечения информационного взаимодействия.

Ключевым элементом информационной инфраструктуры, во многом определяющим ее содержание, являются информационные технологии. Под информационной технологией понимается упорядоченная совокупность методов обработки сообщений, включающих поиск, сбор, хранение, передачу и распространение сообщений, а также их предоставление человеку.

Информационная инфраструктура по форме — это совокупность социально-технических систем, реализующих функции обеспечения информационного взаимодействия, и общественно поддерживаемого порядка использования данных систем в жизни человека и общества.

В информационной инфраструктуре современного общества выделяют три основных сегмента: субъектный, общественный и смешанный.

Субъектный сегмент ориентирован на обеспечение информационного обмена в интересах отдельных субъектов информационной сферы и образуется

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

инфраструктурами сетей связи и информатизации индивидуального пользования. Сети связи представляют собой технологические системы, включающие средства и линии связи и предназначенные для осуществления электросвязи или почтовой связи¹. Понятие «электросвязи» раскрывается в законодательстве как «любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам». Дефиниция «почтовая связь» в законодательстве определена как «вид связи, представляющий собой единый производственно-технологический комплекс технических и транспортных средств, обеспечивающий прием, обработку, перевозку, доставку (вручение) почтовых отправлений, а также осуществление почтовых переводов денежных средств». Особое значение для удовлетворения потребностей общества в информационном обмене имеет федеральная связь, объединяющая все организации и государственные органы, осуществляющие и обеспечивающие электросвязь и почтовую связь на территории Российской Федерации⁴. Можно сказать, что в рамках сети связи сосредоточены все основные технологические средства передачи информации в форме сообщений в интересах граждан, субъектов, представляющих социальные институты общества, государственных органов. Инфраструктура информатизации индивидуального пользования призвана обеспечить «организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов». Она определяется совокупностью информационных технологий, информационных ресурсов и систем, средств, обеспечивающих возможность использования информационных ресурсов и систем субъектами информационной сферы, систем автоматизированного управления, систем автоматизации производства, а

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

также кадров, обеспечивающих их эксплуатацию. При этом технологическую основу инфраструктуры информатизации субъектов составляют информационные ресурсы, информационные технологии и Федеральный закон «О связи» от 18 июня 2003 г. Ст. 2. Там же. Ст. 2. Федеральный закон «О почтовой связи» от 17 июля 1999 г. Ст. 2. А Федеральный закон «О связи» от 18 июня 2003 г. Ст. 11, п. 1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. Ст.

2. телекоммуникационные системы, обеспечивающие возможность удаленного доступа субъектов к информационным ресурсам и системам.

Общественный сегмент информационной инфраструктуры ориентирован на обеспечение информационного обмена в интересах общества и государства и образуется инфраструктурами средств массовой информации и информатизации общего пользования.

Средства массовой информации представляют собой «периодическое печатное издание, радио-, теле-, видеопрограмму, кинохроникальную программу, иную форму периодического распространения массовой информации», т.е. печатных, аудио-, аудиовизуальных и иных сообщений и материалов, предназначенных для неограниченного круга лиц. При этом под массовой информацией понимаются «предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы», а под периодическим печатным изданием — «газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год». Другими словами, средства массовой информации есть издание (радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации), отличающееся наличием трех признаков: постоянным названием, текущим номером и определенной периодичностью выхода в свет.

Средства информатизации общего пользования образуются совокупностью открытых информационных ресурсов библиотек, архивных и музейных фондов, а также открытых государственных информационных

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ресурсов, обеспечивающих свободный доступ граждан к сведениям о деятельности государственных органов, к публикуемым ими нормативным правовым актам и другой общественно значимой информации.

Смешанный сегмент информационной инфраструктуры представляет собой совокупность инфраструктур глобальных информационно-телекоммуникационных систем.

Основной составляющей смешанного сегмента информационной инфраструктуры являются глобальные информационно-телекоммуникационные системы (например, система Интернет) — совокупность средств связи и информатизации, предназначенных как для обеспечения информационного взаимодействия между конкретными субъектами, так и для распространения массовой информации для неограниченного круга лиц.

Функциональные возможности данного сектора информационной инфраструктуры определяются, с одной стороны, имеющимися в его составе средствами получения и передачи сообщений между отдельными субъектами, сбора и хранения полученной информации, а с другой — средствами производства и распространения массовой информации посредством установления информационного взаимодействия отдельного субъекта с неограниченным количеством других субъектов.

Основные сегменты информационной инфраструктуры представлены на рис. 3.

Общей особенностью использования средств информационной инфраструктуры для осуществления информационного взаимодействия является наличие посредника между субъектами, устанавливающими информационное взаимодействие.

В качестве такого посредника могут выступать конкретные физические или юридические лица (посыльный, фельдъегерская служба, телефонная компания), выполняющие функции либо установления информационного взаимодействия, либо предоставления возможности для информационного взаимодействия. Данное обстоятельство обуславливает возникновение

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

определенных общественных отношений между посредником и обслуживаемыми им субъектами.

С появлением электрической связи, развитием глобальных информационно-телекоммуникационных систем функции посредника все больше смещаются в сторону предоставления возможностей информационного взаимодействия.

Таблица 3 - Сегменты информационной инфраструктуры

Сегменты информационной инфраструктуры		
Субъектный	Общественный	Смешанный
Образуются		
инфраструктурами связи и информатизации индивидуального пользования	инфраструктурами СМИ и информатизации общего пользования	инфраструктурами глобальных информационно-коммуникационных систем
Применяются		
для информационного взаимодействия отдельных субъектов	для обеспечения информационного взаимодействия неограниченного круга лиц	для обеспечения информационной деятельности как отдельных субъектов, так и неограниченного круга лиц

Отчетность за занятие

- 1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
- 2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

- 1 Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / пер. под ред. В. Л. Иноземцева. — М., 1999.
- 2 Гейтс Б. Дорога в будущее. — М., 1994.
- 3 Зиновьев А.А. На пути к свсрхобществу. — М.: Центрполиграф, 2000.
- 4 Иноземцев В.Л. К теории постэкономической общественной формации. — М., 1995.
- 5 Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы. — М.: Логос, 2000.
- 6 Тоффлер О. Третья волна. — М., 1995.
- 7 Чоговадзе Г. Г. Информация. Общество. Человек. — М.: Дата+, 2003.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

Для выполнения практического занятия студент должен:

- 1 Ознакомиться с методикой и порядком выполнения работы.
- 2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.
- 3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

~ работать без соответствующего освещения и вентиляции рабочего места;
~ работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
~

передвигаться по рабочему месту без разрешения преподавателя;

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022

~
~
работать в специализированных аудиториях без сменной обуви;
работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Не требуется

Порядок оформления отчета по практическому занятию и его защиты Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

- 1 Что такое информация?
- 2 Каковы основные формы и свойства информации?
- 3 Что такое информационная инфраструктура?
- 4 Каковы основные составляющие информационной инфраструктуры?

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 19.

Система обеспечения информационной безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить теорию обеспечения информационной безопасности организации и Российской Федерации. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

- 1 Обеспечение информационной безопасности организации
- 2 Обеспечение информационной безопасности Российской Федерации

Краткие теоретические или справочно-информационные материалы 1 Обеспечение информационной безопасности предприятия

При всем многообразии видов организаций, направлений и масштабов их деятельности, численности участников **основными объектами обеспечения информационной безопасности**, как правило, являются:

- ~ информация в форме сведений (сведения об участниках организации, о состоянии рынка и ее активов; репутация организации и доброе имя участников организации и т.п.);
- ~ информация в форме сообщений (документы, закрепляющие права собственности организации на материальные и нематериальные активы; документация бухгалтерского учета, налоговые декларации, договоры на выполнение работ и оказание услуг, документация на выпускаемые изделия и т.п.);
- ~ информационная инфраструктура (автоматизированные системы обработки информации и технологического управления, техническое и программное обеспечение информационных и коммуникационных систем и сетей связи, используемых в организации, и т.п.);
- ~ правовой статус организации как субъекта информационной сферы (права на объекты интеллектуальной собственности, на выполнение работ и оказание услуг, на доступ к открытой информации государственных органов, на коммерческую тайну} и т.п., а также обязанности по представлению в уполномоченные государственные органы сведений о результатах экономической деятельности, по соблюдению режима персональных данных, по представлению заинтересованным лицам документов в случае направления заявки на участие в конкурсах и аукционах и т.п.).

Наиболее опасные угрозы безопасности этих объектов проявляются в следующих формах:

- ~ мошенничество, связанное с завладением чужим имуществом или приобретением права на него путем обмана или злоупотребления доверием, основанных на неправомерном доступе к информационно-коммуникационным системам, конфиденциальной информации, на подделке или искажении электронных документов в информационных и коммуникационных системах, сетях следующие:
- ~ клевета, основанная на распространении заведомо ложной информации, порочащей честь и достоинство руководителей организации;
- ~ нарушение авторских и смежных прав, связанных с объектами интеллектуальной собственности;
- ~ шантаж, связанный с угрозой распространения персональных данных, иной информации, охраняемой законом в режиме **тайны**;
- ~ противоправное раскрытие информации ограниченного доступа третьим лицам;
- ~ уничтожение или повреждение информационных ресурсов, информационно-коммуникационных систем и сетей связи посредством использования и распространения вредоносных программ, нарушения правил эксплуатации ЭВМ и их сетей;
- ~ причинение имущественного ущерба собственнику или иному владельцу информационных систем и сетей связи путем обмана или

злоупотребления доверием без признаков хищения.

Владельцы информационных угроз существенно возрастают риски,

Действителен: с 20.08.2021 по 20.08.2022

связанные с осуществлением основной деятельности организации (риск утраты репутации, риск ликвидности, операционные риски, риски утраты собственности или важных **активов** организации). Эти риски связаны с возможностью возникновения ситуаций проявления угроз, требующих дополнительных, часто существенных затрат материальных, людских, **временных**, финансовых и иных ресурсов на ликвидацию **последствий** проявления угроз. Увеличение рисков приводит к увеличению издержек и соответствующему снижению эффективности деятельности организации, уменьшению ее конкурентоспособности.

Система обеспечения информационной безопасности организации характеризуется двумя составляющими: деятельностью по подготовке и реализации мер, направленных на противодействие проявлению угроз информационной безопасности и **минимизацию** последствий этих проявлений; субъектами этой деятельности.

Деятельность по обеспечению информационной безопасности организаций базируется на следующих основных принципах:

- ~ законность, заключающаяся в строгом и неуклонном **исполнении** норм законодательства Российской Федерации, соблюдении прав и свобод человека и гражданина;
- ~ непрерывность, предполагающая рассмотрение деятельности в качестве одной из функций организации;
- ~ комплексность, заключающаяся во всестороннем анализе факторов, оказывающих влияние на риски информационной безопасности, при планировании данной деятельности и использовании всех имеющихся возможностей и выделенных ресурсов для реализации составленных планов;
- ~ замкнутость, заключающаяся в совместном осуществлении деятельности по предупреждению проявления угроз, снижению их опасности, выявлению проявлений угроз, минимизации последствий этих проявлений, а также по оценке эффективности выполнения планов противодействия угрозам и их соответствующего уточнения.

В этой деятельности широко используются методы поощрения, убеждения и принуждения.

Меры по противодействию проявлению угроз информационной безопасности организации и минимизации последствий этих проявлений охватывают три основных направления деятельности:

- ~ управление персоналом;
- ~ организация объектового режима;
- ~ организационно-техническое обеспечение.

Меры по управлению персоналом направлены на минимизацию рисков, связанных с проявлением личностных свойств и качеств участников организации, а также взаимодействующих с ней субъектов. Они включают подбор и расстановку кадров, обеспечение должной мотивации сотрудников к добросовестной работе, подготовку и повышение их квалификации.

Меры по организации объектового режима нацелены на минимизацию рисков, связанных с возможными попытками нанесения ущерба организации ее участникам и взаимодействующим с ней субъектам. Эти мероприятия включают осуществление пропускного и внутриобъектового режимов, в том числе установление и поддержание режимов информации, информационно-коммуникационных систем и систем связи, контроль поддержания установленных режимов и проведение служебных расследований по фактам их нарушения. При этом режимы информационно-коммуникационных систем и систем связи направлены на достижение требуемых значений основных свойств безопасности используемых в организации информационных технологий: конфиденциальности, целостности и готовности к использованию.

Меры по организационно-техническому обеспечению позволяют использовать возможности техники для установления и поддержания объектового режима. Они включают мероприятия по использованию средств защиты информации, информационных и коммуникационных систем, средств связи, а также по установлению и реализации политики безопасности в информационно-коммуникационных системах.

Важную роль в эффективной реализации мер по противодействию угрозам информационной безопасности играет нормативно-методическое обеспечение.

Основными субъектами обеспечения информационной безопасности организаций являются создаваемые в них координационные (например, советы по безопасности информационных технологий) и кадровые органы, специализированные структурные подразделения по вопросам информационной

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

безопасности или должностные лица, а также структурные образования, специализирующиеся на оказании услуг в данной области, объединяемые в единую систему.

Структура указанной системы и ее составных частей может быть различной. Например, в организации может быть создан совет по безопасности информационных технологий, который решает вопросы выработки внутренней политики в этой области, ее реализации и нормативно-методического обеспечения. Для качественного выполнения данных функций в состав совета включают представителей высшего руководства организации и должностных лиц, осуществляющих непосредственное управление обеспечением информационной безопасности. В некоторых случаях управление этой деятельностью может быть возложено на ответственных сотрудников соответствующих структурных подразделений.

2 Обеспечение информационной безопасности Российской Федерации

Осуществление деятельности по обеспечению информационной безопасности Российской Федерации возложено на государство, которое в соответствии с законодательством является основным субъектом обеспечения безопасности.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В соответствии с Доктриной информационной безопасности Российской Федерации национальные интересы в информационной **сфере** включают следующие основные составляющие:

соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

~ потенциала страны;
~ информационное обеспечение государственной политики Рос- сийской Федерации;
~ развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на Мировой рынок;
~ обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
~ защита национальных информационных ресурсов от несанк- ционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

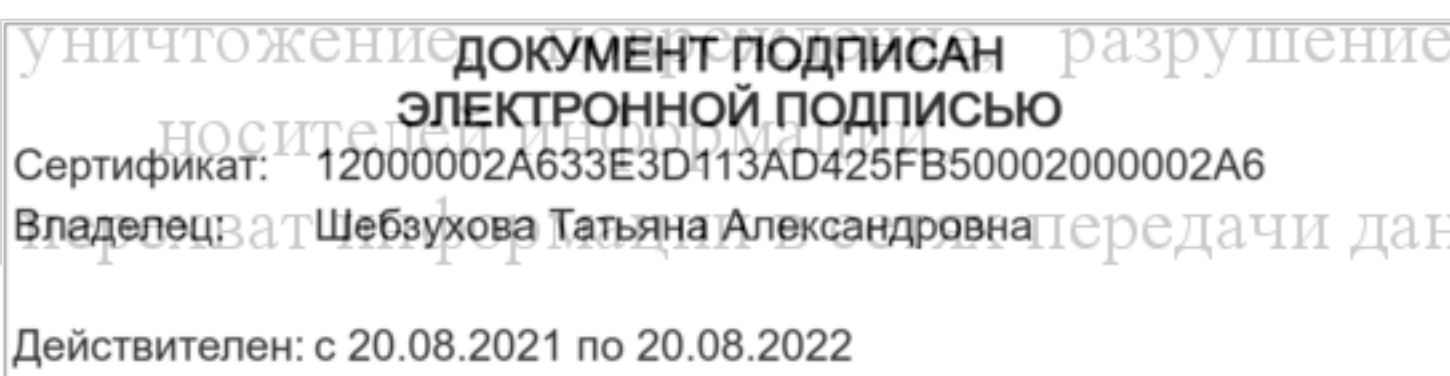
Основными объектами обеспечения информационной безопасности Российской Федерации являются ее национальные интересы:

~ информация в форме сведений (свобода мысли, национальные культурные ценности);
~ информация в форме сообщений (архивные документы; документы, являющиеся музейными предметами или составляющие музейные коллекции; тиражированные документы);
~ информационная инфраструктура (сети связи и инфраструктура информатизации; инфраструктура средств массовой информации и книгоиздания; инфраструктура открытых информационных ресурсов библиотек, архивных и музейных фондов);
~ правовой статус субъектов информационной сферы Российской Федерации (совокупность реальных прав и обязанностей субъектов).

К угрозам информационной безопасности Российской Федерации, в частности, относятся:

~ противодействие реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
~ противоправные сбор и использование информации;
~ разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
~ уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
~ утечка информации по техническим каналам;
~ внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

~ уничтожение документов, разрушение носителей информации, хищение машинных и других документов, документов, содержащих информацию, передачу данных и на линиях связи,



~ дешифрование этой информации и навязывание ложной информации;
~ использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
~ несанкционированный доступ к информации, находящейся в банках и базах данных;
~ нарушение законных ограничений на распространение информации.

Деятельность по обеспечению информационной безопасности Российской Федерации осуществляется на основе принципов, разделяемых на общие и особенные.

К наиболее важным общим принципам деятельности по обеспечению безопасности относятся гуманизм, конкретность, эффективность, сочетание гласности и профессиональной тайны, законность и конституционность.

Принцип гуманизма заключается в обеспечении прав и свобод человека и гражданина при осуществлении противодействия угрозам информационной безопасности, недопущении противоправных посягательств на его личность, унижения чести и достоинства человека, произвольного вмешательства в его частную жизнь, личную и семейную тайны, ограничения свободы его информационной деятельности, а также в минимизации ущерба этим правам и свободам в случаях, когда их ограничение осуществляется **на** законных основаниях.

Принцип конкретности состоит в обеспечении безопасности применительно к конкретным жизненным обстоятельствам с учетом разнообразных форм проявления объективных законов на основе достоверной информации как о внутренних и внешних угрозах, так и о возможностях противодействия им. Достоверная информация позволяет установить конкретные формы проявления угроз, определить в соответствии с этим цели и действия по обеспечению безопасности, конкретизировать методы противодействия угрозам, а также необходимые для их реализации силы и средства.

Принцип эффективности заключается в достижении целей противодействия при наименьших затратах сил и средств. Обеспечение информационной безопасности в любой социальной общности требует

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

определенных материальных, финансовых и людских Ресурсов. Исходя из этого обеспечение безопасности, как и всякая. Общественно полезная деятельность людей, должна осуществляться рационально и эффективно. Обычно критерием эффективности, который применяется на практике, является отношение размера предотвращенного ущерба от реализации угроз к затратам на противодействие этим угрозам.

Принцип сочетания гласности и профессиональной тайны состоит в нахождении и поддержании необходимого баланса между открытостью деятельности по противодействию угрозам информационной безопасности, позволяющей добиться доверия и поддержки общества, и защитой определенной информации, разглашение которой может снизить эффективность противодействия угрозам безопасности.

Принцип законности и конституционности означает осуществление всех свойственных государственным организациям и должностным лицам функций в строгом соответствии с действующей конституцией, законами и подзаконными актами, согласно установленной в законодательном порядке компетенции. Строгое и неуклонное соблюдение законности и конституционности должно быть **непременным требованием, принципом деятельности не только государственных, но и негосударственных органов, учреждений и организаций.**

К числу особенных принципов деятельности по обеспечению информационной безопасности следует отнести, прежде всего, глобальность.

Принцип глобальности заключается в том, что указанная деятельность должна осуществляться согласованно как в конкретном обществе, так и в международном сообществе. К важным формам осуществления деятельности по обеспечению информационной безопасности относится социальное регулирование, в том числе правовые и организационные мероприятия.

Важнейшими формами осуществления деятельности по обеспечению информационной безопасности являются регулятивная и организационная формы.

Регулятивная форма деятельности по обеспечению информационной

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

безопасности характеризуется нормами регулирования общественных отношений по поводу противодействия угрозам и мерами по выработке и поддержанию этих норм. Выделяют два основных типа норм: технические и социальные.

Технические нормы определяют порядок взаимодействия человека с окружающей средой, осуществления деятельности по созданию материальных благ, пользования орудиями труда, в частности средствами и системами информатизации, телекоммуникации и связи. Современную систему технических норм составляют правила использования современных информационных технологий, правила защиты информации и информационных систем от несанкционированного доступа, правила пользования средствами автоматизации управления и обработки информации. Следование этим правилам способствует более производительной и эффективной работе, предупреждает нанесение ущерба таким объектам национальных интересов, как информация и информационно-телекоммуникационные системы, производственный травматизм и заболевания.

Социальные нормы регулируют поведение индивидов и подразделяются на поддерживаемые силами социальной общности без участия государства и на поддерживаемые с использованием государственного принуждения.

Первые включают, прежде всего, мораль, обычаи и традиции, корпоративные и религиозные нормы. Эти нормы играют большую роль в противодействии угрозам сохранения национальной идентичности.

Мораль, или моральные нормы — правила поведения, основанные на представлениях национальной общности о добре и зле, справедливости и несправедливости, честности и бесчестии и других подобных этических качествах. Значительная часть моральных норм вырабатывается и поддерживается нацией в целом или большей частью ее социальных групп.

Под обычаями понимаются правила поведения, сложившиеся в далеком прошлом и поддерживаемые в силу привычки в современном обществе. Норма, ставшая обычаем, оказывает свое регулирующее воздействие в силу ее

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

эмоционального восприятия членами общества, привыкшими к ее соблюдению настолько, что реализация данной нормы превратилась в потребность.

Традиции представляют собой правила поведения, которые определяют порядок, процедуру проведения каких-либо мероприятий, связанных с торжественными или знаменательными, значительными событиями в жизни индивида как представителя конкретной нации, а также другие элементы социального и культурного наследия, передающиеся от поколения к поколению (идеи, Взгляды, вкусы, образ действия и мысли и т. п.).

Широкое распространение в современном обществе получили нормы общественных объединений, политических партий, закрепленные их уставами, — корпоративные нормы. Эти нормы определяют порядок участия членов в деятельности конкретных организаций, их взаимоотношения с руководством, взаимодействие с другими организациями.

Религиозные нормы представляют собой правила, установленные различными вероисповеданиями. Такие нормы содержатся в Библии, Коране, Талмуде и других религиозных книгах либо в сознании верующих, исповедующих языческие, различные культы. Они определяют порядок совершения религиозных обрядов.

Общим для всех этих норм является то, что они, как правило, составляют значительную часть национальных духовных ценно- отличающих одну нацию от другой.

Важной составляющей социального регулирования деятельности по обеспечению информационной безопасности является **праворегулирование общественных отношений**. Оно заключается в установлении определенных правовых норм осуществления наиболее важных общественных отношений и охраны этих норм от нарушения с использованием государственного принуждения. Правовое регулирование отношений в целях обеспечения информационной безопасности осуществляется в рамках правовой деятельности государства, в структуре которой выделяются законодательная (пра- вотворческая), правоприменительная и судебная деятельность.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Законодательная деятельность заключается в подготовке, принятии и издании законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности или минимизации их воздействия на защищаемые общественные отношения. Законодательная деятельность направлена на создание правовой основы выполнения государственными органами задач по противодействию угрозам, на установление таких правил реализации общественных отношений в рассматриваемой области, при которых ни внешние, ни внутренние угрозы не оказывают на защищаемые отношения существенного негативного воздействия. Совокупность нормативных правовых актов, являющихся источниками права в данной сфере, составляют основу так называемого нормативного правового обеспечения информационной безопасности. Правоприменительная деятельность представляет собой основанную на законодательстве оперативную, повседневную реализацию органами исполнительной власти (государственного управления) функций государства в области обеспечения информационной безопасности. Эта деятельность осуществляется в следующих формах:

- подготовка, принятие и исполнение решений органов исполнительной власти об осуществлении конкретных мероприятий по противодействию угрозам информационной безопасности;
- координация деятельности органов исполнительной власти в процессе подготовки и реализации конкретных мероприятий;
- осуществление правоприменительной практики в рассматриваемой области;
- проведение консультативной и информационной деятельности органов исполнительной власти, направленной на создание условий для эффективного выполнения возложенных на эти органы задач;
- выполнение учетной, аналитической, прогнозной и программной работы, административных договоров;
- взаимодействие органов исполнительной власти с другими ветвями и институтами государственной власти в целях согласования усилий по противодействию угрозам;
- информационное обеспечение всех субъектов противодействия

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

- угрозам информационной безопасности в системе исполнительной власти;
- государственный контроль за законностью деятельности субъектов правового регулирования в рассматриваемой области.

Судебная деятельность охватывает реализацию функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам информационной безопасности. Эта деятельность является неотъемлемой составляющей обеспечения информационной безопасности, так как позволяет каждому реализовать свое конституционное право на объективное рассмотрение всех обстоятельств, связанных с применением к нему мер государственного принуждения.

Правовое обеспечение информационной безопасности характеризуется двумя основными составляющими: деятельностью государства по обеспечению информационной безопасности, осуществляемой в правовой форме; органами государственной власти, осуществляющими эту деятельность. Данное правовое обеспечение возникает в процессе взаимодействия права (как средства регулирования общественных отношений) и государства (как основного субъекта противодействия угрозам его безопасности). Правовое обеспечение проявляется в воздействии правовых механизмов на общественные отношения в целях осуществления функций государства по противодействию угрозам безопасности.

Правовое обеспечение информационной безопасности регулирует отношения в области организации противодействия угрозам информационной безопасности как отдельных организаций, так в Российской Федерации в целом, во многом определяя структуру и принципы других видов обеспечения информационной безопасности, в частности организационного обеспечения.

Правовые средства обеспечения информационной безопасности выражаются в установлениях (субъективные права, обязанности, льготы, запреты, поощрения, наказания и т.п.) и деяниях (технологии — акты реализации прав и обязанностей), противодействующих реализуемым в информационной сфере угрозам интересам субъектов права и обеспечивающих достижение

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

социально полезных целей. Они отражают функциональную, прикладную сторону правовой системы, выступают в качестве элементов механизма правового регулирования, во многом определяя эффективность данного механизма.

Организационное обеспечение информационной безопасности состоит в осуществлении планирования и управления материальными, людскими, финансовыми и другими ресурсами государства, выделяемыми для противодействия угрозам. В рамках этой деятельности могут приниматься меры, направленные на развитие научных исследований в области повышения устойчивости информационной инфраструктуры к проявлению угроз, на содействие в установленном законодательством порядке работе общественных организаций, ставящих своей целью противодействие угрозам информационной безопасности и определение форм возможного взаимодействия с ними, на согласование деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в области противодействия угрозам, на развитие системы массовой информации, способной удовлетворять потребности граждан в актуальных, достоверных сведениях об интересующих их событиях общественной жизни, обеспечивать их своевременное поступление к гражданам и т.д.

Организационное обеспечение информационной безопасности Российской Федерации осуществляется с использованием средств технического, кадрового, материального, финансового, информационного и научного обеспечения.

Средства технического обеспечения информационной безопасности образуются совокупностью технических и программных средств защиты информации, предотвращения несанкционированного доступа в информационные, телекоммуникационные и вычислительные системы и сети связи, а также методического обеспечения их использования.

Средства кадрового обеспечения информационной безопасности характеризуются программами подготовки кадров по различным аспектам данной деятельности, а также используемыми учебными и методическими

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

материалами.

Средства материального обеспечения характеризуются совокупностью объектов, выделяемых для размещения средств технологического обеспечения, сил, участвующих в обеспечении информационной безопасности, средств организации их деятельности и т.п.

Средства финансового обеспечения представляют собой совокупность экономических инструментов получения, привлечения, перераспределения и использования денежных средств для решения задач обеспечения информационной безопасности.

Средства информационного обеспечения образуются совокупностью информационных фондов и банков данных, используемых в процессе решения задач обеспечения информационной безопасности, а также средств их актуализации.

Средства научного обеспечения информационной безопасности определяются совокупностью научных теорий, концепций, категорий, закономерностей и методов, предназначенных для изучения процессов и явлений развития информационной сферы общества, угроз национальным интересам, реализуемым в этой сфере, и для противодействия этим угрозам.

Общая структура средств обеспечения информационной безопасности представлена на рис. 7.

Основные субъекты обеспечения информационной безопасности Российской Федерации объединены в рамках государственной системы защиты информации.

К их числу относятся:

- службы контроля, надзора и обеспечения информационной безопасности государственных органов;
- специализированные предприятия и организации, осуществляющие деятельность в области разработки средств и предоставления услуг по защите информации;
- сертификационно-испытательные центры;
- аттестационные центры;
- службы безопасности и защиты информации предприятий и организаций, осуществляющих обработку персональных данных, Конфиденциальной информации и информации, составляющей

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

государственную тайну.

Таблица 6 - Средства обеспечения информационной безопасности

Средства обеспечения информационной безопасности			
Правовые	Политически е	Организационные	
Совокупность правовых механизмов противодействия проявлениям угроз национальным интересам в информационной сфере	Совокупность средств борьбы за государственную власть и использования государственной власти для противодействия угрозам информационной безопасности	Мероприятия, осуществляемые субъектами обеспечения информационной безопасности	
		технологические	материальные
		кадрового обеспечения	финансовые
		научного обеспечения	информационного обеспечения

Отчетность за занятие

- 1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
- 2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

- 1 Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования. — М.: Институт социальной информатики, 1999.
 - 2 Гейтс Б. Дорожка к будущему. — М.: 1994.
 - 3 Владелец: Шебзухова Татьяна Александровна
 - 4 Действителен: с 20.08.2021 по 20.08.2022
- М., 1995.

- 5 *Иноземцев В.Л.* Современное постиндустриальное общество: природа, противоречия, перспективы. — М.: Логос, 2000.
- 6 *Тоффлер О.* Третья волна. — М., 1995.
- 7 *Чоговадзе Г. Г.* Информация. Общество. Человек. — М.: Дата+, 2003.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

Для выполнения практического занятия студент должен:

- 1 Ознакомиться с методикой и порядком выполнения работы.
- 2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.
- 3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- ~ работать без соответствующего освещения и вентиляции рабочего места;
- ~ работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- ~ передвигаться по аудитории без разрешения преподавателя;
- ~ работать в специализированных аудиториях без сменной обуви;
- ~ работать на одном рабочем месте более двух человек.

- 4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.
- 5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	12000002A633E3D113AD425FB50002000002A6
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 20.08.2021 по 20.08.2022	

Не требуется

Порядок оформления отчета по практическому занятию и его защиты Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

- 1 Раскройте содержание обеспечения информационной безопасности организации.
- 2 Перечислите наиболее важные объекты информационной безопасности организации и угрозы безопасности этих объектов.
- 3 Опишите структуру системы обеспечения информационной безопасности организации.
- 4 Раскройте содержание информационной безопасности Российской Федерации.
- 5 Перечислите наиболее важные объекты информационной безопасности Российской Федерации и основные угрозы их безопасности.
- 6 Перечислите принципы обеспечения информационной безопасности Российской Федерации и раскройте их содержание.
- 7 Перечислите основные виды обеспечения информационной безопасности и раскройте их содержание.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 20.

Организационные структуры системы обеспечения безопасности информации

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить организационные структуры государственной системы обеспечения информационной безопасности. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти

2 Организационные структуры системы обеспечения информационной безопасности предприятия (организации)

Краткие теоретические или справочно-информационные материалы 1
Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Наиболее развитой составляющей отечественного комплекса обеспечения информационной безопасности является **государственная система защиты информации**, в составе которой можно выделить такие **типовые организационные структуры**, как: службы контроля, надзора и обеспечения безопасности органов исполнительной власти; специализированные предприятия и организации — лицензиаты в различных областях компетенции уполномоченных органов исполнительной власти, которые являются разработчиками средств и поставщиками услуг по защите информации; сертификационно-испытательные центры; аттестационные центры; службы безопасности и защиты информации предприятий и организаций, независимо от их формы собственности.

Службы контроля и надзора органа исполнительной власти *не*сут основную нагрузку по формированию и развитию системы защиты информации в соответствующем органе власти. Такие службы входят в состав административного аппарата органов исполнительной власти и, как правило, в их функции входят:

- ~ разработка нормативно-методических документов отраслевого (ведомственного) уровня по выполнению требований обеспечения безопасности и защиты информации;
- ~ разработка, организация и проведение контрольных и надзорных мероприятий в пределах установленной сферы компетентности органа государственной власти и оформление результатов ^проведения таких мероприятий;
- ~ - выдача предписаний об устранении нарушений требований - Нормативных документов;
- ~ подготовка мотивированных предложений о полном или частичном прекращении деятельности подведомственных организаций в случае, если иными мерами нарушения требований нормативных документов не могут быть устранены;
- ~ проведение в ходе государственного контроля (надзора) разъяснительной работы по выполнению требований нормативных актов в области обеспечения безопасности и защиты информации.

Выполнение указанного перечня функций обеспечивают специалисты, соответствующие следующей **номенклатуре основных должностей**: руководитель управления, службы; руководитель отдела, сектора; специалист по направлению деятельности службы безопасности; инженер-метролог (нормоконтролер технической и организационно-распорядительной

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

документации).

Особое место в государственной системе защиты информации занимают **специализированные предприятия — разработчики комплексов и средств обеспечения**, а также поставщики услуг в области безопасности и защиты информации. Именно от степени их развития, уровня и качества поставляемой продукции и услуг зависит безопасность, устойчивость и надежность функционирования всей инфраструктуры информационной безопасности. Поэтому недаром одним из обязательных требований к указанным предприятиям и организациям является лицензирование их деятельности уполномоченным органом исполнительной власти в соответствии с законодательством о государственном регулировании отдельных видов деятельности.

Предлагаемые на рынке этими предприятиями **услуги организационно-технологического характера** можно классифицировать в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности:

~ **обследование** — услуга, которая может включать анализ защищенности используемых информационных технологий, обследование системы документооборота, обследование организации в целом (т.е. анализ влияния существующего документооборота на защищенность бизнес-процессов), проверку деятельности организации в соответствии с требованиями нормативно-правовых документов и тому подобное;

~ **проектирование комплексной системы обеспечения**, при котором должен быть охвачен не только технический уровень, но и все механизмы защиты, включая организационно-правовые;

~ **внедрение системы защиты информации** на договорной основе с использованием специализированных подрядных организаций, имеющих соответствующую лицензию (может дать большой эффект за счет высокой квалификации привлекаемых специалистов);

~ **сопровождение систем информационной безопасности и работ по защите информации третьими лицами (аутсорсинг)**, т.е. оказание специализированной оперативной помощи в случае внештатных ситуаций, периодическое обновление специального и общесистемного программного обеспечения в случае появления новых атак и уязвимостей.

Организация и технологии разработки специализированных комплексов, систем и средств защиты информации принципиально не отличаются от используемых в других отраслях создания высокотехнологичной продукции, в частности средств вычислительной техники. Основная номенклатура

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

должностей традиционна для высокотехнологичных предприятий: конструктор по наладке и испытаниям; конструктор по стандартизации; программист; технолог; электроник; техник по наладке и испытаниям.

Бурный процесс информатизации и, как следствие, все возрастающая актуальность обеспечения требований информационной безопасности приводят к необходимости видоизменения и дополнения номенклатуры специалистов. Широкое распространение общепризнанной международной практики проведения такого вида услуги, как аудит информационной безопасности, привело к появлению специалистов нового профиля — аудиторов, которые осуществляют свою деятельность в соответствии с рекомендациями **отечественных и международных стандартов**. К таким стандартам относятся:

~ ГОСТ Р ИСО/МЭК 17799—2005 «Информационная технология — Практические правила управления информационной безопасностью»;

~ ИСО/МЭК 17799—2000 «Информационная технология. Кодекс установившейся практики для менеджмента информационной безопасности»;

~ В5 7799 «Управление информационной безопасностью. Практические правила»;

~ вторая часть В5 7799-2:2002 «Системы управления информационной безопасностью — спецификация с руководством по использованию».

Сертификационно-испытательные центры и лаборатории занимают особое место среди предприятий и организаций — лицензиатов в области обеспечения безопасности и защиты информации. Эти организационные структуры обеспечивают необходимую поддержку такой функции государственно-общественного регулирования в области информационной безопасности, как сертификацию средств и оценки качества оказания услуг по защите /информации.

Наряду с лицензированием своей деятельности в области защиты информации указанные центры и лаборатории должны пройти дополнительно обязательную организационно-правовую процедуру — аккредитацию в качестве сертификационно-испытательных структур, которая в настоящее время осуществляется исключительно уполномоченными органами исполнительной власти. Реформа законодательства о техническом регулировании пока не дает четкой правовой основы использования обязательной сертификации как

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

механизма независимого подтверждения качества продукции и услуг в области информационной безопасности, но и не отменяет возможность применения такого механизма, по крайней мере в системе сертификации продукции, работ и услуг, средств и комплексов защиты сведений, составляющих государственную тайну. Нарботанные практикой за более чем десятилетний период организационно-технологические процедуры в целом могут также с успехом применяться в системах добровольной сертификации. Поэтому существующие сертификационно-испытательные центры (лаборатории) по-прежнему будут играть ключевую роль в процессах подтверждения соответствия средств, комплексов и систем защиты установленным требованиям по безопасности информации. Номенклатура указанных должностей подобных структур также может быть дополнена новой категорией специалистов, например, «оценщик», или специалист по оценке защищенности информационных технологий, предусмотренной стандартом ГОСТ Р ИСО/МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий».

Аттестационные центры наряду с сертификацией средств, работ и услуг в области обеспечения информационной безопасности осуществляют относительно похожие процедуры подтверждения соответствия, называемые аттестацией объектов информатизации.

Как правило, по объему и характеру работ традиционные аттестационные центры (лаборатории) не имеют существенных отличительных особенностей по сравнению с сертификационно-испытательными центрами, а наиболее известные отечественные компании — поставщики услуг в области защиты информации — имеют аккредитацию по обоим видам деятельности и, соответственно, примерно одинаковую номенклатуру основных должностей.

Активно развивается также рынок образовательных услуг в области информационной безопасности по повышению квалификации специалистов, руководителей служб безопасности, руководителей IT-подразделений, пользователей средств защиты, так как необходимым условием для получения лицензии на деятельность в области защиты информации является наличие

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

персонала необходимого уровня квалификации и подготовки. Однако система дополнительного образования в области информационной безопасности пока находится в стадии формирования, что затрудняет выделение ее типовых элементов.

Службы безопасности и защиты информации предприятий и организаций независимо от вида деятельности и форм собственности являются самой распространенной организационной структурой в рассматриваемой области общественной деятельности и по существу составляют основу всей системы обеспечения информационной безопасности предприятий, организаций и страны в целом. Поэтому целесообразно рассмотреть вопросы их функционирования более подробно.

Непосредственная деятельность по организации функционирования и эксплуатации комплексов обеспечения информационной безопасности осуществляется штатными специалистами соответствующих структурных подразделений. Они должны иметь определенную квалификацию в соответствии с требованиями, установленными номенклатурой должностей и служащих. Типовые требования можно найти в квалификационном справочнике должностей руководителей, специалистов и других служащих, утвержденном Министерством труда и социального развития Российской Федерации в 2003 г.

2 Организационные структуры системы обеспечения информационной безопасности предприятия (организации)

Задачи и функции организационных структур, осуществляющих реализацию специальных защитных мероприятий (служб безопасности) на уровне предприятия (организации), определяются потребностями реальных бизнес-процессов, их спецификой и масштабами.

Традиционной задачей служб безопасности хозяйствующих субъектов является обеспечение так называемой физической защиты, под которой подразумевается охрана имущества, материальных и финансовых ценностей, а также в отдельных случаях защита персонала, прежде всего руководства, от

преступных посягательств. Для решения этой задачи **служба безопасности** должна обеспечить выполнение следующих **функций**:

- организацию пропускного режима, разграничение физического доступа на защищаемые объекты;
- организацию инженерно-технической защиты охраняемых зданий и помещений объекта;
- обнаружение проникновения внешнего нарушителя на охраняемую территорию и принятие соответствующих мер противодействия;
- противодействие противоправным действиям внутренних нарушителей по отношению к имуществу и активам предприятия;
- организацию личной охраны персонала.

Менее традиционной является **задача обеспечения безопасности управления бизнес-процессами**, включающая защиту нематериальных активов и информационных ресурсов предприятия (информационная безопасность) и участие в управлении персоналом в части обеспечения лояльности и благонадежности.

Реализация талой задачи **подразумевает выполнение следующих функций**:

- разведка и контрразведка, в том числе изучение криминальных аспектов рынка, организация противодействия экономическому шпионажу, сбор на законных основаниях информации о деловых партнерах и других лицах, имеющих контакты с предприятием;
- организация противодействия недобросовестной конкуренции, выявление фактов противоправного использования нематериальных активов и интеллектуальной собственности;
- организация секретного и конфиденциального делопроизводства и ведения конфиденциальных переговоров;
- обеспечение безопасности автоматизированных информационных технологий, а также информации, циркулирующей в компьютерных сетях;
- противодействие технической разведке, т.е. способам несанкционированного съема информации с помощью технических средств;
- проведение служебных расследований обстоятельств разглашения сведений, составляющих коммерческую тайну и т.д.;
- оценка лояльности и благонадежности персонала путем проведения в рамках, установленных законом, оперативно-розыскных мероприятий и выявление неблагонадежных сотрудников (группы риска) с помощью различных методов тестирования;
- подготовка персонала, в том числе нештатных сотрудников, формирование правосознания и культуры поведения всех сотрудников предприятия по вопросам обеспечения его безопасности;
- оценка эффективности работы структурных подразделений,

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

входящих в состав службы безопасности и защиты информации.

В случае **создания полномасштабной собственной системы безопасности и защиты информации** наиболее эффективной является трехуровневая структура стратегического, тактического и оперативного управления.

На уровне стратегического управления осуществляется формулирование конкретных интересов предприятия, его бизнес-процессов и критериев обеспечения их защищенности, выделение необходимого ресурсного обеспечения. Очевидно, что решение этих задач должно быть сосредоточено на уровне высшего руководства, в структуре топ-менеджмента предприятия, где происходит утверждение соответствующей концепции развития предприятия. Тактическое управление осуществляет руководитель службы безопасности или должностное лицо, на которое возложены соответствующие обязанности, его заместители и руководители структурных подразделений. Основная задача тактического управления — формирование корпоративной нормативно-методической базы требований по обеспечению безопасности, их реализация и контроль за их выполнением. Оперативное управление включает практическую реализацию защитных функций, в том числе эксплуатацию специализированных технических средств и проведение организационных процедур, и осуществляется как штатными, так и нештатными сотрудниками службы безопасности, выполняющими соответствующие функции наряду с основной деятельностью.

Полномасштабный комплекс обеспечения безопасности предприятия включает следующие штатные и нештатные структуры:

- ~ совет или комиссии по различным вопросам обеспечения
- ~ безопасности, возглавляемые топ-менеджментом предприятия;
- ~ руководство службой безопасности и руководимые им кон-
- ~ сультативно-экспертные группы;
- ~ охрannое подразделение;
- ~ инженерно-техническое подразделение;
- ~ аналитическую группу;
- ~ подразделение секретного делопроизводства и ведения кон-
- ~ фиденциальных переговоров;

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

- ~ подразделение противодействия технической разведке и технической защиты информации;
- ~ подразделение администрирования информационно-управляющих систем по требованиям безопасности информации;
- ~ подразделение оценки лояльности и благонадежности персонала, его подготовки в области обеспечения безопасности;
- ~ подразделение аудита систем обеспечения безопасности и оценки их эффективности.

Конкретная реализация структуры службы безопасности находится в компетенции первого руководителя предприятия. Номенклатура штатных и нештатных должностей службы безопасности на уровне предприятия может включать все перечисленные должности специализированных организационных структур. Кроме этого, в подразделениях системы управления предприятием, не связанных напрямую с обеспечением безопасности, на практике часто вводится штатная либо нештатная должность администратора информационной безопасности. Основной обязанностью такого специалиста является обеспечение защиты информационных ресурсов и администрирование соответствующих средств защиты Информации на уровне конкретного подразделения.

Для малых предприятий с небольшими объемами бизнеса и численностью работников обязанности по выполнению ряда вышеперечисленных функций возлагаются на отдельных ответственных сотрудников. На предприятиях среднего масштаба создается отдельное относительно небольшое подразделение, координирующее и контролирующее выполнение функций по обеспечению безопасности другими подразделениями предприятия. Крупные фирмы и корпорации развивают службу безопасности до полномасштабной структуры, имеющей все необходимые полномочия и ресурсы для решения поставленных задач.

При этом следует иметь в виду, что выполнение охранных функций, в том числе защиту личного состава, в соответствии с действующим законодательством могут осуществлять либо вневедомственная охрана МВД России, либо частные охранные предприятия, действующие на основе законодательства о частной детективной и охранной деятельности. Частным охранным предприятиям разрешается оказывать различные услуги, в том числе

по вооруженной охране имущественных ценностей при транспортировке и по защите жизни и здоровья персонала. Кроме этого, охранные предприятия обеспечивают проектирование, монтаж и обслуживание средств охранно-пожарной сигнализации, консалтинговые услуги по вопросам правомерной защиты от противоправных посягательств.

Другой пример использования услуг третьих лиц по обеспечению требований информационной безопасности характерен для предприятий и организаций негосударственных форм собственности, не имеющих собственных подразделений по защите государственной тайны. По действующему законодательству они в случае необходимости могут заключать с государственными организациями договоры об использовании их режимно-секретных органов (РСО), обеспечивающих секретное делопроизводство и режимные мероприятия в соответствии с лицензией на проведение работ с использованием сведений, составляющих государственную тайну, и на оказание услуг по защите указанных сведений.

В ходе информатизации малые и средние предприятия все чаще используют такую форму договорных услуг, как аутсорсинг информационных технологий, включая вопросы обеспечения информационной безопасности.

Одной из распространенных форм организационного обеспечения безопасности предприятия, отражающей комплексный характер рассматриваемой проблемы и один из методов ее решения, является создание отдельных комиссий. Такие штатные структуры выполняют на временной или постоянной основе отдельные экспертные или контрольно-ревизионные функции по обеспечению безопасности, в частности инвентаризацию имущественных ценностей, нематериальных активов и информационных ресурсов, экспертизу материалов, подготовленных к публикации в средствах массовой информации, аттестацию персонала. Включение в комиссии сотрудников различных подразделений структуры управления предприятием позволяет скоординировать их взаимодействие и в целом повысить эффективность совместной деятельности.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

Решение задачи физической защиты предполагает проведение следующих специальных мероприятий и действий сотрудников службы по организации режимов обеспечения безопасности объекта:

- ~ определение и категорирование охраняемых зон по уровню доступа;
- ~ разработка заданий на укрепление периметров охраняемых зон (ограждение, решетки, замки и т.д.), контроль проектирования системы укрепления периметра, прием и контроль хода эксплуатации системы;
- ~ определение точек доступа в охраняемые зоны, разработка заданий по их оборудованию необходимыми техническими средствами, контроль проектирования и эксплуатации технических средств, разработка инструкций о порядке пропускного и внутриобъектового режимов;
- ~ разработка заданий по применению средств охранно-пожарной сигнализации, систем видеонаблюдения, автоматизированных систем ограничения и контроля доступа в охраняемые зоны, прием и контроль эксплуатации;
- ~ согласование порядка выноса (вноса) из охраняемых зон материальных ценностей и других видов ресурсов;
- ~ разработка заданий, контроль проектирования, прием и контроль эксплуатации систем специальной связи, оборудования комнат и порядка приема посетителей;
- ~ категорирование информационных ресурсов по степени секретности и конфиденциальности как нормативной основы ограничения их обращения;
- ~ определение возможных физических каналов утечки информации с ограниченным доступом, разработка заданий на проектирование систем противодействия технической разведке, прием и контроль их эксплуатации;
- ~ разработка порядка проведения служебных расследований по фактам нарушения пропускного и внутриобъектового режимов, а также взаимодействия с правоохранительными органами.

Указанные мероприятия позволяют обеспечить реализацию такой важной характеристики защищенности, как **конфиденциальность информации**, путем использования тех или иных технологий ограничения доступа. Однако, как правило, решение проблемы повышения эффективности бизнес-процессов требует увеличения их открытости, непротиворечивости как для внешней среды, так и для собственного управленческого персонала. Это позволяет в максимальной степени обеспечить масштабность производственной деятельности, ее настройку на быстро изменяющиеся условия рыночной и политической конъюнктуры. Поэтому не менее важными, а подчас и более актуальными задачами обеспечения информационной безопасности являются повышение доступности

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

и целостности информационных активов корпорации в условиях бурного внедрения компьютерных технологий. Реализация всех характеристик защищенности является также необходимым условием обеспечения качества бизнес-процессов за счет поддержания их непрерывности, под которой понимается и своевременное принятие управленческих решений.

Отчетность за занятие

- 1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
- 2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

- 1 *Возжеников А. В.* Национальная безопасность: теория, политика, стратегия. — М.: РАГС, 1998.
- 2 Основы национальной безопасности России / под ред. В. Л. Манилова. — М.: Друза. 1998.
- 3 *Прохожее А.А.* Национальная безопасность: основы теории, сущность, проблемы. — М.: РАГС, 1997.
- 4 *Прохожее А.А.* Человек и общество: законы социального развития и безопасности. — М.: РАГС, 2002.
- 5 *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

- 1 Для выполнения практического занятия студент должен:
- 2 Ознакомиться с методикой и порядком выполнения работы.

