

УТВЕРЖДАЮ
 Декан факультета

 (подпись) Матвеев П.В.
 ФИО
 «___» _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	О Естественнонаучный
Выпускающая кафедра	О7 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	О7 Информационные системы и программная инженерия

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
4	7	3	108	34	17	0	17	74	0	0	74	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

09.03.02 Информационные системы и технологии

год набора группы: 2024

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Шимкун Вячеслав Владиславович, преподаватель

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-2.18 — Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Формированию компетенций служит достижение следующих результатов образования:

ПСК-2.18

знания:

Основные понятия в области защиты и обработки конфиденциальных документов;

Особенности нормативно-правовой организации конфиденциального делопроизводства;

Угрозы безопасности информации при организации конфиденциального документооборота;

Понятие, задачи и виды контроля исполнения конфиденциальных документов;

умения:

Разрабатывать требования к автоматизированным системам обработки и хранения конфиденциальных документов;

навыки:

Навыки анализа комплекса мер по информационной безопасности в системах документационного обеспечения управления.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**.

Содержание дисциплины является основой для освоения дисциплин: **ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-3 — Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ПК-94 — способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач
- ПСК-2.9 — Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Лекции	Практические занятия		ПСК-2.18
4	7	Раздел 1. Основы организации конфиденциального делопроизводства и учета конфиденциальных документов. Нормативно-правовые основы организации конфиденциального делопроизводства. Специфика технологии конфиденциального документооборота. Учет конфиденциальных документов.	31	9	5	4	22	30
4	7	Раздел 2. Организация обработки конфиденциальных документов. Обработка входящих конфиденциальных документов. Обработка исходящих и внутренних конфиденциальных документов. Порядок работы исполнителей с конфиденциальными документами. Организация контроля исполнения конфиденциальных документов. Размножение конфиденциальных документов.	36	10	6	4	26	30
4	7	Раздел 3. Организация хранения конфиденциальных документов и дел. Систематизация и оперативное хранение конфиденциальных документов и дел. Архивное хранение конфиденциальных документов и дел. Организация проверки наличия и уничтожения конфиденциальных документов. Основы организации защищенного электронного документооборота.	41	15	6	9	26	40
Всего за 7 семестр			108	34	17	17	74	100
Всего по дисциплине			108	34	17	17	74	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Основы организации конфиденциального делопроизводства и учета конфиденциальных документов.	Практическая работа №1 – «Анализ деятельности организации»	4
2	Раздел 2. Организация обработки конфиденциальных документов.	Практическая работа №2 – «Разработка порядка работы с конфиденциальными документами»	4
3	Раздел 3. Организация хранения конфиденциальных документов и дел.	Практическая работа №3 – «Разработка частной политики ИБ по организации конфиденциального документооборота»	9
Всего за 7 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Основы организации конфиденциального делопроизводства и учета конфиденциальных документов.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
2		Подготовка к практической работе №1, оформление отчета.	16
3	Раздел 2. Организация обработки конфиденциальных документов.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
4		Подготовка к практической работе №2, оформление отчета.	20
5	Раздел 3. Организация хранения конфиденциальных документов и дел.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
6		Подготовка к практической работе №3, оформление отчета.	20

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
7						ДР				ДР				Отч. по ПЗ		ДР	диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- диф. зач. – дифференцированный зачет.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. Г. Серго, В. С. Пуцин. . Основы права интеллектуальной собственности для ИТ-специалистов. М.: Интернет-Университет Информационных Технологий, 2011, 13 экз.
2. А. Г. Серго, В. С. Пуцин. . Основы права интеллектуальной собственности для ИТ-специалистов. М.: Интернет-Университет Информационных Технологий, 2011, эл. рес.
3. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
4. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
5. И. Н. Кузнецов. . Документационное обеспечение управления. Документооборот и делопроизводство. Москва: Юрайт, 2022, эл. рес.
6. И. О. Косых, Л. Б. Кочин. . Методы защиты информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2017, эл. рес.
7. С. А. Клейменов, В. П. Мельников, А. М. Петраков. . Администрирование в информационных системах. М.: Академия, 2008, 30 экз.
8. С. А. Клейменов, В. П. Мельников, А. М. Петраков. . Администрирование в информационных системах. М.: Академия, 2008, эл. рес.
9. С. Н. Никифоров. . Методы защиты информации. Защита от внешних вторжений. Санкт-Петербург: Лань, 2022, эл. рес.

5.2. Дополнительная литература по дисциплине:

1. М. В. Кирсанова, Н. Н. Анодина, Ю. М. Аксёнов. . Деловая переписка. М.: ИНФРА-М, 2006, 3 экз.
2. М. Ю. Рогожин. Делопроизводство. Организация архива предприятия. СПб.: Питер, 2005, 3 экз.
3. Ю. М. Дёмин. Делопроизводство. Подготовка служебных документов. СПб.: Питер, 2006, 3 экз.

5.3. Периодические издания:

не требуются.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <http://e.lanbook.com/> — ЭБС Лань;;
2. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;;
3. <https://scholar.google.com/> — Академия Google;
4. <http://library.voenmeh.ru/jirbis2/> — Р“Р»Р°РІРSP°СЦ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voennemeh.ru/jrbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/> - КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. LibreOffice;
2. Linux.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. LibreOffice;
3. Linux.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *О Естественнотехнический БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ПСК-2.18 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

Содержание дисциплины охватывает круг вопросов, связанных с основными понятиями документооборота, с организацией защищенного документооборота, а также с порядком хранения, обработки и уничтожения конфиденциальных документов.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены лекционные занятия (**17 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**74 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 34 ч. аудиторных занятий, и 74 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Основы организации конфиденциального делопроизводства и учета конфиденциальных документов.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Ю. М. Дёмин. Делопроизводство. Подготовка служебных документов: СПб.: Питер, 2006 (1-3) И. О. Косых, Л. Б. Кочин. . Методы защиты информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2017 (1) С. Н. Никифоров. . Методы защиты информации. Защита от внешних вторжений: Санкт-Петербург: Лань, 2022 (1-3)	6
Подготовка к практической работе №1, оформление отчета.	И. Н. Кузнецов. . Документационное обеспечение управления. Документооборот и делопроизводство: Москва: Юрайт, 2022 (1-3) М. В. Кирсанова, Н. Н. Анодина, Ю. М. Аксёнов. . Деловая переписка: М.: ИНФРА-М, 2006 (1)	16
Итого по разделу 1		22
Раздел 2. Организация обработки конфиденциальных документов.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	М. Ю. Рогожин. Делопроизводство. Организация архива предприятия: СПб.: Питер, 2005 (1-4) А. Г. Серго, В. С. Пушин. . Основы права интеллектуальной собственности для ИТ-специалистов: М.: Интернет-Университет Информационных Технологий, 2011 (4) А. Г. Серго, В. С. Пушин. . Основы права интеллектуальной собственности для ИТ-специалистов: М.: Интернет-Университет Информационных Технологий, 2011 (4) С. А. Клейменов, В. П. Мельников, А. М. Петраков. . Администрирование в информационных системах: М.: Академия, 2008 (4)	6
Подготовка к практической работе №2, оформление отчета.	Ю. М. Дёмин. Делопроизводство. Подготовка служебных документов: СПб.: Питер, 2006 (1-3) С. А. Клейменов, В. П. Мельников, А. М. Петраков. . Администрирование в информационных системах: М.: Академия, 2008 (4)	20
Итого по разделу 2		26
Раздел 3. Организация хранения конфиденциальных документов и дел.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	И. О. Косых, Л. Б. Кочин. . Методы защиты информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2017 (2) С. А. Клейменов, В. П. Мельников, А. М. Петраков. .	6

Подготовка к практической работе №3, оформление отчета.	<p>Администрирование в информационных системах: М.: Академия, 2008 (4)</p> <p>И. Н. Кузнецов. . Документационное обеспечение управления. Документооборот и делопроизводство: Москва: Юрайт, 2022 (1-2)</p> <p>Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2)</p> <p>С. А. Клейменов, В. П. Мельников, А. М. Петраков. . Администрирование в информационных системах: М.: Академия, 2008 (4)</p> <p>Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2)</p> <p>С. Н. Никифоров. . Методы защиты информации. Защита от внешних вторжений: Санкт-Петербург: Лань, 2022 (3-4)</p> <p>Ю. М. Дёмин. Делопроизводство. Подготовка служебных документов: СПб.: Питер, 2006 (1-4)</p>	20
	Итого по разделу 3	26

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- отчет по практическому заданию;
- дифференцированный зачет.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Отчет по практическому заданию

К каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При выполнении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждой ПЗ.

ПЗ считается выполненным и защищенным успешно при условии:

- наличия программного приложения, реализующего поставленную задачу;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие программного приложения указанным требованиям, его работоспособность и эффективность – 7 баллов;
- отчет оформлен полностью в соответствии с ГОСТ 7.32-2017 – 3 балла;
- правильность ответов на вопросы – 7 баллов;
- своевременность выполнения и защиты индивидуального задания – 3 балла.

Основанием для снижения количества баллов являются:

- несоответствие программного приложения указанным требованиям, его неэффективность или некорректная работа;
- оформление отчета не соответствует ГОСТ 7.32-2017 в 3 и более пунктах;
- неверные ответы на вопросы или отсутствие ответов;
- несвоевременность выполнения и защиты индивидуального задания.

В случае, если ПЗ и отчет к нему выполнены своевременно в соответствии с указанными требованиями, а также получены правильные ответы на вопросы при его защите студент получает максимальное количество баллов – 20. Для того, чтобы ПЗ было сдано, требуется набрать 12 баллов.

Дифференцированный зачет

График контрольных мероприятий предусматривает выполнение студентом 3 заданий, каждое из которых может быть оценено максимально на 20 баллов.

Дифференцированный зачет выставляется по сумме результатов контрольных мероприятий, проводимых в течение семестра. Максимальная сумма баллов за семестр – 60 баллов. Набранная итоговая сумма баллов пересчитывается в оценку по следующей схеме: - 56 – 60 баллов – отлично; - 51 – 55 балла - хорошо; - 40 – 50 баллов – удовлетворительно, меньше 40 - не зачтено.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ПСК-2.18	
4	7	Раздел 1. Основы организации конфиденциального делопроизводства и учета конфиденциальных документов.	31	9	5	4	22	30	Отчет по практическому заданию
4	7	Раздел 2. Организация обработки конфиденциальных документов.	36	10	6	4	26	30	Отчет по практическому заданию
4	7	Раздел 3. Организация хранения конфиденциальных документов и дел.	41	15	6	9	26	40	Отчет по практическому заданию
Всего за 7 семестр			108	34	17	17	74	100	
Всего по дисциплине			108	34	17	17	74	100	

Критерии оценивания

ПСК-2.18

- Вопросы открытого типа:*
- № 1 *Информация это -*
- № 2 *Под информационной безопасностью понимается...*
- № 3 *комплекс мероприятий, направленных на обеспечение информационной безопасности это...*
- № 4 *Доступность – это...*
- № 5 *Конфиденциальность – это...*
- № 6 *Угроза – это...*
- № 7 *попытка реализации угрозы это...*
- № 8 *нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций это...*
- № 9 *Ошибка – это...*
- № 10 *Сбой – это...*
- Вопросы закрытого типа:*
- № 1 *Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется*
- достоверной
 - конфиденциальной
 - документированной
 - коммерческой тайной
- № 2 *По принадлежности информационные ресурсы подразделяются на*
- государственные, коммерческие и личные
 - государственные, не государственные и информацию о гражданах
 - информацию юридических и физических лиц
 - официальные, гражданские и коммерческие
- № 3 *К конфиденциальной информации относятся документы, содержащие*
- государственную тайну
 - законодательные акты
 - "ноу-хау"
 - сведения о золотом запасе страны
- № 4 *Запрещено относить к информации ограниченного доступа*
- информацию о чрезвычайных ситуациях
 - информацию о деятельности органов государственной власти
 - документы открытых архивов и библиотек
 - все, перечисленное в остальных пунктах
- № 5 *Какая информация подлежит защите?*
- информация, циркулирующая в системах и сетях связи
 - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
 - только информация, составляющая государственные информационные ресурсы

- любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
- № 6 От чего зависит информационная безопасность?
- А) от компьютеров
 - Б) от поддерживающей инфраструктуры
 - В) от информации
- № 7 Основные составляющие информационной безопасности:
- А) целостность
 - Б) достоверность
 - В) конфиденциальность
- № 8 Природа происхождения угроз:
- А) случайные
 - Б) преднамеренные
 - В) природные
- № 9 Предпосылки появления угроз:
- А) объективные
 - Б) субъективные
 - В) преднамеренные
- № 10 Источник угрозы – это...
- А) потенциальный злоумышленник
 - Б) злоумышленник
 - В) нет правильного ответа