

УТВЕРЖДАЮ
 Декан факультета

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление/специальность подготовки	09.03.04 Программная инженерия
Специализация/профиль/программа подготовки	Разработка программно-информационных систем
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	
3	6	4	144	34	17	0	17	110	0	0	110	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

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

09.03.04 Программная инженерия

год набора группы: 2024

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Шимкун Вячеслав Владиславович, старший 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 ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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:

ОПК-3 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПСК-1/23.4 — способность использовать различные технологии разработки программного обеспечения

Формированию компетенций служит достижение следующих результатов образования:

ОПК-3

знания:

- основные стандарты в области информационной безопасности;
- современные методы защиты и средства реализации методов в сетях передачи данных и переработки информации;
- современные методы кодирования и шифрования;
- методы аутентификации в современных операционных системах и специальные средства защиты информации;
- классификация компьютерных систем по уровню защищенности;
- программные механизмы и методы реализации систем защиты информации;
- классификация угроз;;

умения:

- применять действующую законодательную базу в области обеспечения информационной безопасности;

навыки:

- использовать нормативные документы в профессиональной деятельности;
- поиска нормативной правовой информации, необходимой для профессиональной деятельности;
- работы с нормативными правовыми актами;.

ПСК-1/23.4

знания:

- различия защиты физической, организационной, математической и программной;
- модели и методы построения защищенных систем обработки информации;
- реализация механизмов разграничения доступа пользователей к ресурсам распределенной системы обработки информации или компьютерной сети;
- методы организации защищенных каналов передачи информации через компьютерные сети общего пользования;
- принципы формирования политики информационной безопасности;;

умения:

- применять полученные знания в практике построения защищенных систем обработки информации, включая конфиденциальную информацию и обработку персональных данных;;

навыки:

- выявлять угрозы информационной безопасности объекта;.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.04 Программная инженерия*.

Содержание дисциплины является логическим продолжением дисциплин: **ПРАВОВЕДЕНИЕ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**.

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

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-2 — Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
- 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
- УК-10 — Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
- УК-2 — Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 з.е., 144 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		ОПК-3	ПСК-1/23.4
3	6	Раздел 1. Нормативно-правовая основа концепции ИБ. Правовые, нормативные и организационно-распорядительные документы. Обзор Российского законодательства в области информационной безопасности. Обзор Международного законодательства в области информационной безопасности. Модель процесса управления ИБ в разрезе различных стандартов. Требования стандарта ISO/ IEC 27000 к системам информационной безопасности. Требования нормативных стандартов к оценке рисков ИБ.	46	10	5	5	36	34	32
3	6	Раздел 2. Правовое обеспечение информационной безопасности. Основные понятия о нормах, правах и правовых отношениях. Содержание и структура правового обеспечения. Правовая база защиты информации. Правовая база защиты персональных данных. Законодательная база в области интеллектуальной собственности. Законодательная база в области электронной подписи. Законодательная база в области технического регулирования.	48	12	6	6	36	34	32
3	6	Раздел 3. Организационное обеспечение информационной безопасности. Основные понятия о нормах, правах и правовых отношениях. Содержание и структура правового обеспечения. Правовая база защиты информации. Правовая база защиты персональных данных. Законодательная база в области интеллектуальной собственности. Законодательная база в области электронной подписи. Законодательная база в области технического регулирования Политика ИБ. Организационная система подготовки кадров в области обеспечения ИБ . Разработка организационных структур для систем информационной безопасности. Разработка Политик ИБ. Разработка организационного обеспечения для управления рисками ИБ.	50	12	6	6	38	32	36
Всего за 6 семестр			144	34	17	17	110	100	100
Всего по дисциплине			144	34	17	17	110	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Нормативно- правовая основа концепции ИБ.	Нормативно-правовая основа концепции ИБ. Изучение типовых форм правовых, нормативных и организационно- распорядительных документов .	5
2	Раздел 2. Правовое обеспечение информационной безопасности.	Правовое обеспечение информационной безопасности. Изучение законодательная базы в области электронной подписи и защиты информационной безопасности.	3
3		Правовое обеспечение информационной безопасности. Разработка содержания и структуры правового обеспечения на примере конкретной организации.	3
4	Раздел 3. Организационное обеспечение информационной безопасности.	Организационное обеспечение информационной безопасности. Разработка системы организационного обеспечения информационной безопасности для конкретного предприятия (организации).	3
5		Организационное обеспечение информационной безопасности. Разработка Политики ИБ для конкретной организации, предприятия.	3
Всего за 6 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Нормативно-правовая основа концепции ИБ.	Нормативно-правовая основа концепции ИБ. Работа с лекционным материалом. Подготовка к практическим занятиям.	36

2	Раздел 2. Правовое обеспечение информационной безопасности.	Правовое обеспечение информационной безопасности. Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту.	36
3	Раздел 3. Организационное обеспечение информационной безопасности.	Организационное обеспечение информационной безопасности. Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту.	38
Всего за 6 семестр			110

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
6					Отч. по ПЗ	ДР			Отч. по ПЗ	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. Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности. Москва: Юрайт, 2020, эл. рес.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

1. Кадровое дело;
2. Моделирование и анализ информационных систем.

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

1. <http://library.voenmeh.ru/jirbis2/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. <https://urait.ru/> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
3. <http://e.lanbook.com/> — ЭБС Лань;
4. <http://www.intuit.ru/department/security/secbasics/> — НОУ ИНТУИТ | Основы информационной безопасности | Информация;
5. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация.

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.voenmeh.ru/jirbis2/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.

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.

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 **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.04 Программная инженерия*. Дисциплина реализуется на факультете *О Естественнотехнический БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ОПК-3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПСК-1/23.4 способность использовать различные технологии разработки программного обеспечения.

Содержание дисциплины охватывает круг вопросов, связанных с правовыми аспектами информационной безопасности, нормативными актами и положениями Российской Федерации в отношении информационной безопасности, обеспечением режимов секретности в организациях.

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 **4 з.е., 144 ч.** Программой дисциплины предусмотрены лекционные занятия (**17 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**110 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 ч., из них 34 ч. аудиторных занятий, и 110 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. Нормативно-правовая основа концепции ИБ.		
Нормативно-правовая основа концепции ИБ. Работа с лекционным материалом. Подготовка к практическим занятиям.	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (5, 6, 7)	36
Итого по разделу 1		36
Раздел 2. Правовое обеспечение информационной безопасности.		
Правовое обеспечение информационной безопасности. Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту.	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (1, 4, 7)	36
Итого по разделу 2		36
Раздел 3. Организационное обеспечение информационной безопасности.		
Организационное обеспечение информационной безопасности. Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту.	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (1, 2, 3, 7)	38
Итого по разделу 3		38

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 каждой ПР 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 ПР.

ПР считается выполненным и защищенным успешно при условии:

- наличия программного приложения, реализующего поставленную задачу;
- наличия отчета;
- защиты ПР по комплекту тестовых вопросов для защиты ПР, 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 ПР 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 ПР была сдана, требуется набрать 12 баллов.

Дифференцированный зачет

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4. Зачёт проводится в виде собеседования. Два основных вопроса и один дополнительный в случае, если ответы студента на первые два не позволяют однозначно определиться с оценкой. Студенты должны продемонстрировать знание и понимание теоретического материала курса.

При выполнении и защите всех практических работ предусмотрена отметка "зачтено-хорошо" по результатам работы в семестре.

Зачтено-отлично:

- все задачи практики решены полностью,
- в процессе собеседования студент продемонстрировал полное знание вопросов.

Зачтено-хорошо:

- все задачи практики решены полностью,
- в процессе собеседования студент продемонстрировал в целом достаточно полное знание вопросов, но допускал мелкие неточности в формулировках ответов.

Зачтено-удовлетворительно:

- все задачи практики решены полностью
- в процессе собеседования студент продемонстрировал удовлетворительное знание вопросов, но допускал неполные ответы, затруднялся в формулировках ответов.

Не зачтено:

- не все задачи практики решены,
- в процессе собеседования студент продемонстрировал неудовлетворительное знание вопросов.

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		ОПК-3	ПСК-1/23.4	
3	6	Раздел 1. Нормативно-правовая основа концепции ИБ.	46	10	5	5	36	34	32	Отчет по практическому заданию
3	6	Раздел 2. Правовое обеспечение информационной безопасности.	48	12	6	6	36	34	32	Отчет по практическому заданию
3	6	Раздел 3. Организационное обеспечение информационной безопасности.	50	12	6	6	38	32	36	Отчет по практическому заданию
Всего за 6 семестр			144	34	17	17	110	100	100	
Всего по дисциплине			144	34	17	17	110	100	100	

Критерии оценивания

ОПК-3

	<i>Вопросы открытого типа:</i>
№ 1	Государственная тайна это:
№ 2	Что можно отнести к правовым мерам ИБ?
№ 3	Что можно отнести к организационным мерам ИБ?
№ 4	Что можно отнести к техническим мерам ИБ?
№ 5	Что такое компьютерный вирус?
№ 6	Основные типы компьютерных вирусов:
№ 7	Ответьте на вопрос «Что называется вирусной атакой?»
№ 8	Программные средства защиты можно разделить на:
№ 9	Наибольшую угрозу для безопасности сети представляют:
№ 10	Технические каналы утечки информации делятся на...
	<i>Вопросы закрытого типа:</i>
№ 1	Разместите средства защиты по группам: 1. Формальные средства защиты: 2. Неформальные средства защиты: 1. Физические средства 2. Аппаратные средства 3. Программные средства 1. Законодательные средства 2. Организационные средства 3. Морально-этические средства 3. Антивирусные средства 3. Религиозные средства
№ 2	В 1975 году Джерри Зальцер и Майкл Шрёдер в статье «Защита информации в компьютерных системах» впервые предложили разделить нарушения безопасности на три основных категории. Позднее эти категории получили краткие наименования: С – I – А – Целостность Авторизованность Интегральность Безопасность Безнаказанность Конфиденциальность

№ 3	Санкционированность
	Доступность
	Защищённость
№ 4	Характер происхождения угроз:
	1. Умышленные факторы.
	2. ... факторы.
	Неумышленные
	Естественные
	Фантастические
	Противоестественные
	Потусторонние
	Сверхестественные
	Целостность можно подразделить на _____ (понимаемую как неизменность информационных объектов) и _____ (относящуюся к корректному выполнению сложных действий (транзакций)).
№ 5	холодную
	неизменную
	горячую
	ликвидную
	корректную
	динамическую
	статическую
	транзакционную
	изменяемую
	Виды угроз. Основные нарушения:
	1. Физической целостности (уничтожение, разрушение элементов).
	2. _____ целостности (разрушение логических связей).
	3. Содержания (изменение блоков информации, внешнее навязывание ложной информации).
	4. Конфиденциальности (разрушение защиты, уменьшение степени защищенности информации).
	5. Прав собственности на информацию (несанкционированное копирование, использование).
	Логической

- Двоичной
- Программной
- Криптографической
- Шестнадцатеричной
- Духовной
- № 6 Концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:
- [1] защищать?
 - от [2] защищать?
 - [3] защищать?
- [1] – **что** / зачем / на какие деньги
- [2] – **чего (кого)** / чего / кого
- [3] –
- как**
- / кем / с чем
- № 7 Ущерб может быть [1] или [2].
- [1] – приемлемым, моральным, финансовым, репутационным
- [2] - моральным, финансовым, репутационным, неприемлемым
- № 8 Чем отличаются информационная безопасность, защита информации и уровень защищенности?
1. Информационная безопасность – это ...
 2. Уровень защищенности – это ...
 3. Защита информации – это ...
- А - одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным уровнем защищенности.
- Б - процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.
- В - состояние защищенности информации и поддерживающей инфраструктуры. Правильно укажите соответствие средств защиты их определениям.
- № 9
1. Формальные средства защиты

2. Неформальные средства защиты

А – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

Б – регламентируют деятельность человека.

В – выполняют защитные функции без заранее предусмотренной процедуры
№ 10 Доступность информации – это

свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними.

свойство системы обеспечивать доступ субъектов к информации.

свойство информации быть понятной человеку с недостаточным уровнем образования и (или) интеллекта.

свойство системы осуществлять своевременный информационный обмен между субъектами информационной системы.

свойство системы сохранять стоимость доступа к информации на уровне или ниже прожиточного минимума.

ПСК-1/23.4

Вопросы открытого типа:

- № 1 **Интернет — браузеры предназначены:**
- № 2 **Веб — страницы передаются по этому протоколу:**
- № 3 **Описать функции современных вычислительных сетей и основные прикладные аспекты их использования**
- № 4 **Назовите определение IP-адреса.**
- № 5 **Назовите определение маршрутизатора (коммутатора).**
- № 6 **Какие сетевые серверы бывают?**
- № 7 **Как называется комбинация IP-адреса и номера порта?**
- № 8 **Расшифруйте аббревиатуру «СЗИ».**
- № 9 **Что такое «аудит» в контексте информационной безопасности?**
- № 10 **Расшифруйте аббревиатуру «ИСПД».**

Вопросы закрытого типа:

- № 1 Выберите утверждение, соответствующее виду ЭЦП.

1. Усиленная неквалифицированная электронная подпись.
2. Простая электронная подпись.
3. Усиленная квалифицированная электронная подпись.

А - Она тождественна собственноручной.

№ 2	Б - Это сочетание логина и пароля.
	В - Подлинность подписи и неизменность документа подтверждается квалифицированным сертификатом.
	Г - Она надежнее простой ЭП, но, по своей сути, тождественна собственноручной.
	Д - Это сочетание логина и пароля или SMS-код подтверждения.
	Распределите средства антивирусной защиты (САВЗ) по типам.
	1. САВЗ типа «А»
	2. САВЗ типа «Б»
	3. САВЗ типа «В»
	4. САВЗ типа «Г»
	А - Предназначены для применения на автономных автоматизированных рабочих местах (АРМ) .
№ 3	Б - Предназначены для применения на автоматизированных рабочих местах (АРМ) информационных систем.
	В - Предназначены для применения на серверах информационных систем.
	Г - Предназначены для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем - серверах, автоматизированных рабочих местах (АРМ).
	Какие из перечисленных САВЗ имеют сертификат ФСТЭК и официально продаются на российском рынке?
	Avast
	Trend Micro
	McAfee
	Dr.Web
	ESET NOD32
	Panda

AVG

Norton

№ 4 Kaspersky
Для чего нужна машиночитаемая доверенность (МЧД)?

Чтобы подписывать документы своей ЭЦП от лица организации и руководителя выдавших доверенность.

Чтобы подписывать документы своей ЭЦП.

Чтобы подписывать документы ЭЦП руководителя от его лица.

Чтобы подписывать документы ЭЦП руководителя от лица организации выдавшей доверенность.

№ 5 Чтобы подписывать документы ЭЦП руководителя.
Что должен иметь каждый компьютер или принтер подключённый к локальной сети:

1. сетевой адаптер
2. маршрутизатор
3. коммутатор

№ 6 Сеть, объединяющая несколько компьютеров и позволяет использовать ресурсы компьютеров и подключённых к сети периферийных устройств, называется:

1. замкнутая
2. региональная
3. локальная

№ 7 Протоколом является:

1. устройство для работы локальной сети
2. стандарт отправки сообщений через электронную почту
3. стандарт передачи данных через компьютерную сеть

№ 8 Основными видами компьютерных сетей являются сети:

№ 9

1. клиентские, корпоративные, международные
2. локальные, глобальные, региональные
3. социальные, развлекательные, бизнес-ориентированные

Обобщённая геометрическая характеристика компьютерной сети - это:

№ 10

1. Топология сети
2. Сервер сети
3. Удалённость компьютеров сети

Протокол компьютерной сети - совокупность:

1. Электронный журнал для протоколирования действий пользователей сети
2. Технических характеристик трафика сети
3. Правил, регламентирующих приём-передачу, активацию данных в сети