

УТВЕРЖДАЮ
Декан факультета

_____ Матвеев П.В.

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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	
3	6	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: 2025

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 — 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-2.1 — Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации

Формированию компетенций служит достижение следующих результатов образования:

ОПК-3

знания:

знать основы организационной и правовой защиты информации, ее современные проблемы и терминологию;

умения:

умение использовать специализированную терминологию;

навыки:

навык использования нормативных документов в профессиональной деятельности.

ПК-2.1

знания:

нормативные правовые акты в области защиты информации;

национальные, межгосударственные и международные стандарты в области защиты информации;

руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.;

умения:

определять цели проведения аудита;

моделировать угрозы;

применять необходимые инструментальные средства;

оформлять документацию по этапам аудита информационной безопасности.;

навыки:

разработка аналитического обоснования необходимости создания системы защиты информации в организации..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

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-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 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		ОПК-3	ПК-2.1
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.	35	10	5	5	25	34	34
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.	37	12	6	6	25	34	34
3	6	Раздел 3. Организационное обеспечение информационной безопасности. 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.	36	12	6	6	24	32	32
Всего за 6 семестр			108	34	17	17	74	100	100
Всего по дисциплине			108	34	17	17	74	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.	25
2	Раздел 2. Правовое обеспечение информационной безопасности.	Правовое обеспечение информационной безопасности. Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту.	25

3	Раздел 3. Организационное обеспечение информационной безопасности.	Организационное обеспечение информационной безопасности. Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту.	24
Всего за 6 семестр			74

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://e.lanbook.com/> — ЭБС Лань;
2. <http://www.intuit.ru/departments/security/secbasics/> — НОУ ИНТУИТ | Основы информационной безопасности | Информация;
3. <http://www.intuit.ru/departments/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
4. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;
5. <http://library.voenmeh.ru/jirbis2/> — 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.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 *09.03.02 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*:

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-2.1 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации.

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 **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. 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)	25
Итого по разделу 1		25
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)	25
Итого по разделу 2		25
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)	24
Итого по разделу 3		24

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	ПК-2.1	
3	6	Раздел 1. Нормативно-правовая основа концепции ИБ.	35	10	5	5	25	34	34	Отчет по практическому заданию
3	6	Раздел 2. Правовое обеспечение информационной безопасности.	37	12	6	6	25	34	34	Отчет по практическому заданию
3	6	Раздел 3. Организационное обеспечение информационной безопасности.	36	12	6	6	24	32	32	Отчет по практическому заданию
Всего за 6 семестр			108	34	17	17	74	100	100	
Всего по дисциплине			108	34	17	17	74	100	100	

**Оценочные материалы по дисциплине ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

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

- № 1 Прочитайте текст и запишите развернутый обоснованный ответ
Объясните принципы классификации информации и её уровней защищённости в организации.
- № 2 Прочитайте текст и запишите развернутый обоснованный ответ
Охарактеризуйте процесс разработки организационной структуры службы ИБ в крупной компании.
- № 3 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие формы ответственности за нарушение ИБ предусмотрены в РФ?
- А. Уголовная
- В. Административная
- С. Дисциплинарная
- Д. Гражданско-правовая
- № 4 Прочитайте текст и установите последовательность
Укажите порядок этапов аттестации рабочего места по 152-ФЗ:
- А. Сбор заявки от пользователя
- В. Тестирование средств защиты
- С. Оформление заключения
- Д. Установка требуемого ПО
- № 5 Прочитайте текст и установите последовательность
Установите последовательность действий при расследовании утечки ПДн:
- А. Идентификация инцидента
- В. Сбор журналов доступа
- С. Проведение интервью
- Д. Анализ собранной информации
- № 6 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой орган в РФ отвечает за контроль соблюдения 152-ФЗ?
- А. ФСТЭК
- В. Роскомнадзор
- С. Минцифры
- Д. МВД
- № 7 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие уровни доступа существуют при работе с ПДн?
- А. Общий доступ
- В. Ограниченный доступ

С. Персональный доступ

Д. Временный доступ

- № 8 Прочитайте текст и установите соответствие
Соотнесите нормативный акт и вид аккредитации:

Акт

Аккредитация

А. Приказ ФСТЭК №17

1. На соответствие ISO/IEC 27001

В. ГОСТ Р ИСО/МЭК 27001

2. На соответствие требованиям ФСТЭК

С. Приказ Минцифры №356

3. Аккредитация УЦ для подготовки специалистов ИБ

Д. Приказ Минпромторга №123

- № 9 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой федеральный закон устанавливает требования к защите персональных данных?

А. 149-ФЗ «Об информации»

В. 152-ФЗ «О персональных данных»

С. 63-ФЗ «Об электронной подписи»

Д. 184-ФЗ «О техническом регулировании»

- № 10 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой документ определяет структуру СУИБ в соответствии с ISO/IEC 27001?

А. Политика информационной безопасности

В. Стандарт ISO/IEC 27005

С. Положение о доступе

Д. Руководство по эксплуатации системы

- № 11 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие методы управления рисками ИБ входят в качественный подход?

А. SWOT-анализ

В. Расчёт ожидаемых потерь

С. Матричное ранжирование

Д. Экспертные интервью

- № 12 Прочитайте текст и установите соответствие

Договор

Цель

А. NDA (Non-Disclosure Agreement)

1. Взаимное понимание намерений при сотрудничестве

В. SLA (Service Level Agreement)

2. Определение уровня услуг ИБ-сервиса

С. MOU (Memorandum of Understanding)

3. Защита коммерческой и конфиденциальной информации

Д. SPY (Service Provisioning Yearly)

ПК-2.1 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать

участие в проведении экспериментальных исследований системы защиты информации

- № 1 Прочитайте текст и запишите развернутый обоснованный ответ
Объясните ключевые положения Закона «Об электронной подписи» (63-ФЗ) в контексте ИБ.
- № 2 Прочитайте текст и установите соответствие
Соотнесите стадию внедрения СУИБ и ключевую задачу:
- | Стадия | Задача |
|-----------------|-------------------------------------------------------|
| А. Инициация | 1. Формирование целевых показателей и сбор требований |
| В. Реализация | 2. Оценка соответствия и корректировка |
| С. Мониторинг | 3. Внедрение политик, процессов и технологий |
| Д. Планирование | |
| Е. Аудит | |
- № 3 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие документы входят в правовую основу ИБ в организации?
- А. Федеральные законы
 - В. Региональные постановления
 - С. Внутренние регламенты
 - Д. Международные конвенции
- № 4 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие принципы заложены в стандарте ISO/IEC 27001?
- А. PDCA
 - В. Контроль доступа
 - С. Ротация персонала
 - Д. Управление рисками
- № 5 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие организационные меры применяются при внедрении СУИБ?
- А. Разработка позиций и ролей
 - В. Закупка антивирусов
 - С. Обучение сотрудников
 - Д. Проведение внутренних аудитов
- № 6 Прочитайте текст и установите последовательность
Расположите шаги методики качественной оценки рисков:
- А. Интервью с экспертами
 - В. Определение критериев уровня риска
 - С. Составление матрицы рисков
 - Д. Приоритизация рисков
- № 7 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой уровень секретности присваивается стратегическим оборонным планам?

- A. Конфиденциально
- B. Секретно
- C. Совершенно секретно
- D. Особой важности

№ 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой документ регламентирует выдачу допуска к гостайне?

- A. 152-ФЗ
- B. Приказ ФСТЭК №17
- C. Постановление №1119
- D. Указ Президента о гостайне

№ 9 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой принцип ИБ означает, что сотрудник имеет только минимально необходимые для работы права?

- A. Разделение функций
- B. Минимизация прав
- C. Целостность
- D. Конфиденциальность

№ 10 Прочитайте текст и установите соответствие

Соотнесите подразделение ФСТЭК и область ответственности:

Подразделение	Область
A. Лаборатория	1. Надзор за исполнением требований 149-ФЗ и 152-ФЗ
B. Экспертный совет	2. Разработка методик и рекомендаций
C. Контрольный орган	3. Испытания и аттестация технических средств ИБ
D. Отдел лицензирования	

№ 11 Прочитайте текст и запишите развернутый обоснованный ответ

Раскройте содержание международного стандарта ISO/IEC 27005 по управлению рисками ИБ.

№ 12 Прочитайте текст и установите последовательность

Установите правильную последовательность при подготовке к сертификации по ISO/IEC 27001:

- A. Определение области СУИБ
- B. Проведение GAP-анализа
- C. Внедрение недостающих контролей
- D. Внутренний аудит