



Автономная некоммерческая организация высшего образования
«Волгоградский институт бизнеса»

Рабочая программа учебной дисциплины

Основы информационной безопасности

(Наименование дисциплины)

15.03.06 Мехатроника и робототехника, направленность (профиль) «Мехатроника»

(Направление подготовки / Профиль)

Бакалавр

(Квалификация)

Кафедра разработчик

Экономики и управления

Год набора

2027

Вид учебной деятельности	Трудоемкость (объем) дисциплины
	Очная форма
	д
Зачетные единицы	3
Общее количество часов	108
Аудиторные часы контактной работы обучающегося с преподавателями:	32
– Лекционные (Л)	16
– Практические (ПЗ)	
– Лабораторные (ЛЗ)	16
– Семинарские (СЗ)	
Самостоятельная работа обучающихся (СРО)	40
К (Р-Г) Р (П) (+;-)	
Тестирование (+;-)	
ДКР (+;-)	
Зачет (+;-)	
Зачет с оценкой (+;- (Кол-во часов))	
Экзамен (+;- (Кол-во часов))	+ (36)

Волгоград 2026

Содержание

Раздел 1. Организационно-методический раздел	3
Раздел 2. Тематический план.....	5
Раздел 3. Содержание дисциплины.....	6
Раздел 4. Организация самостоятельной работы обучающихся	8
Раздел 5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся	10
Раздел 6. Оценочные средства промежуточной аттестации (с ключами)	13
Раздел 7. Перечень учебной литературы, необходимой для освоения дисциплины	16
Раздел 8. Материально-техническая база и информационные технологии	17
Раздел 9. Методические указания для обучающихся по освоению дисциплины	18

Раздел 1. Организационно-методический раздел

1.1. Цели освоения дисциплины

Дисциплина «**Основы информационной безопасности**» входит в **обязательную часть** дисциплин подготовки обучающихся по направлению подготовки **15.03.06 Мехатроника и робототехника, направленность (профиль) «Мехатроника»**

Целью дисциплины является формирование **компетенций** (в соответствии с ФГОС ВПО и требованиями к результатам освоения образовательной программы (ОПОП ВО)):

ОПК-6. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

Дескрипторы общепрофессиональных компетенции:

ОПК-6.1. Способен решать задачи, связанные с обеспечением информационной безопасности, обеспечение приватности данных, а также аудит алгоритмов на предмет уязвимостей.

ОПК-6.2. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с использованием сетевых технологий, включая работу с открытыми репозиториями кода, специализированными базами научных публикаций и др. источниками данных.

Перечисленные компетенции формируются в процессе достижения **индикаторов достижения компетенций:**

Обобщенная трудовая функция/ трудовая функция	Код и наименование дескриптора компетенций	Код и наименование индикатора достижения компетенций (из ПС)
	ОПК-6.1. Способен решать задачи, связанные с обеспечением информационной безопасности, обеспечение приватности данных, а также аудит алгоритмов на предмет уязвимостей. ОПК-6.2. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с использованием сетевых технологий, включая работу с открытыми репозиториями кода, специализированными базами научных публикаций и др. источниками данных.	Знает ИД-1 ОПК-6.1 Методы и средства обеспечения информационной безопасности, обеспечение приватности данных и проведение аудита алгоритмов на предмет уязвимостей (без привязки к профессиональному стандарту) ИД-2 ОПК-6.2 Основы информационной и библиографической культуры, технологии работы с открытыми репозиториями кода, специализированными базами научных публикаций и др. источниками данных (без привязки к профессиональному стандарту) Умеет ИД-3 ОПК-6.1 Решать задачи, связанные с обеспечением информационной безопасности, обеспечение приватности данных и проведение аудита алгоритмов на уязвимости (без привязки к профессиональному стандарту) ИД-4 ОПК-6.2 Решать стандартные задачи профессиональной деятельности на основе информационной и

		библиографической культуры с использованием сетевых технологий, включая работу с открытыми репозиториями, базами научных публикаций и др. источниками данных (без привязки к профессиональному стандарту) Имеет навыки ИД-5 ОПК-6.1 Владение навыками обеспечения информационной безопасности, обеспечение приватности данных и проведение аудита алгоритмов на уязвимости (без привязки к профессиональному стандарту) ИД-6 ОПК-6.2 Владение навыками информационной и библиографической культуры, использования сетевых технологий для работы с открытыми репозиториями кода, базами научных публикаций и др. источниками данных (без привязки к профессиональному стандарту)
--	--	--

1.2. Место дисциплины в структуре ОПОП ВО
направления подготовки 15.03.06 Мехатроника и робототехника, направленность (профиль)
«Мехатроника»

№	Предшествующие дисциплины (дисциплины, изучаемые параллельно)	Последующие дисциплины
1	Основы информационной безопасности	Автоматические системы обеспечения техносферной безопасности

Последовательность формирования компетенций в указанных дисциплинах может быть изменена в зависимости от формы и срока обучения, а также преподавания с использованием дистанционных технологий обучения.

1.3. Нормативная документация

Рабочая программа учебной дисциплины составлена на основе:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки **15.03.06 Мехатроника и робототехника, направленность (профиль) «Мехатроника»**;
- Учебного плана направления подготовки **15.03.06 Мехатроника и робототехника, направленность (профиль) «Мехатроника»** 2027 года набора;
- Образца рабочей программы учебной дисциплины (приказ № 27-О от 01.02.2021 г.).

**Раздел 2. Тематический план
Очная форма обучения (полный срок)**

№	Тема дисциплины	Трудоемкость				Код индикатора и дескриптора достижения компетенций
		Всего	Аудиторные занятия		СРО	
			Л	ПЗ (ЛЗ, СЗ)		
1	2	3	4	5	6	7
1	Основные понятия информационной безопасности и защиты информации	14	4	4	6	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
2	Политика информационной безопасности	10	2	2	6	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
3	Стандарты информационной безопасности	10	2	2	6	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
4	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	10	2	2	6	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
5	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	10	2	2	6	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
6	Инженерно-техническая защита информации	10	2	2	6	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
7	Организационно-правовое обеспечение защиты информации	8	2	2	4	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
Вид итогового контроля (Экзамен)		36				
Итого		108	16	16	40	

Раздел 3. Содержание дисциплины

3.1. Содержание дисциплины

Тема 1. Основные понятия информационной безопасности и защиты информации.

Основные термины и определения. Обеспечение информационной безопасности компьютерных систем. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной (случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные

Тема 2. Политика информационной безопасности

Основные понятия политики безопасности. Структура политики безопасности. Разработка политики организации безопасности организации.

Тема 3. Стандарты информационной безопасности

Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем Министерства обороны США – «Оранжевая книга». Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности. Канадские критерии безопасности компьютерных систем. ГОСТ Р ИСО/МЭК 15408-2002, как аутентичный вариант общих критериев безопасности ИТ. Функциональные требования безопасности. Требования доверия к безопасности. Стандарты ISO/IEC 17799: 2002 (BS 7799:2000). Стандарты по менеджменту информационной безопасности ISO/IEC 27001-27040. Немецкие стандарты BSI. Стандарты SysTrust, SCORE, GIAC. Стандарты для беспроводных сетей. Отечественные стандарты информационной безопасности. Стандарты обеспечения информационной безопасности организаций банковской системы. Российской Федерации. ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2 – 2018. Стандарты информационной безопасности в Интернете (IETF, RFC)

Тема 4. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ

Органы, обеспечивающие национальную безопасность РФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления в области защиты информации в РФ. Тенденции развития информационной политики государств и ведомств. Государственная тайна.

Тема 5. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности

Общие положения. Концептуальные документы в области информационной безопасности. Важнейшие федеральные нормативные правовые акты. Законы, касающиеся охраны интеллектуальной собственности. Положения Гражданского кодекса РФ по защите информации. Международное сотрудничество. Кодекс об административных правонарушениях. Уголовный кодекс и защита информации. Основные подзаконные акты в области информационной безопасности. Указы Президента РФ, постановления Правительства РФ, ведомственная нормативная база.

Тема 6. Инженерно-техническая защита информации

Понятие криптографии. Критерий надежности шифрования. Основные криптографические приемы: блочное шифрование, схема поточного шифрования. Симметричные криптосистемы шифрования. Ассиметричные криптосистемы шифрования. Функции хэширования. Основные процедуры цифровой подписи. Управление криптоключами. Идентификация, аутентификация и управление доступом: методы аутентификации, использующие пароли, строгая аутентификация, биометрическая аутентификация. Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок Особенности взаимодействия с программно- аппаратными средствами защиты. Методика применения средств борьбы с вредоносными закладками на этапе эксплуатации систем. Системы разграничения доступа и защиты от ВЗ. Предупреждение и минимизация последствий воздействия ВЗ. Краткая характеристика мер защиты: юридические, административные и организационные, аппаратно-программные. Компьютерные вирусы. Классификация. Жизненный цикл. Основные каналы распространения вирусов и других

вредоносных программ. Средства борьбы с вирусами: краткая характеристика популярных антивирусных программ. Средства защиты от копирования. Примеры средств и технологий. Вопросы правовой защиты

Тема 7. Организационно-правовое обеспечение защиты информации

Сущность и роль организационно-правовых аспектов информационной безопасности. Человек как главное звено в системе защиты информации и как злоумышленник. Нормативная правовая база информационной безопасности. Закон РФ “Об информации, информационных технологиях и о защите информации”. Виды и категории информации ограниченного доступа: государственная и другие виды тайн. Закон РФ “О государственной тайне”, “О коммерческой тайне”, “О персональных данных”, “О национальной платежной системе”, “О безопасности критической информационной инфраструктуры Российской Федерации”. Государственная система лицензирования и сертификации деятельности в области защиты информации. Указ Президента РФ “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации”. Закон РФ “Об электронной цифровой подписи”. Уголовно- правовое регулирование защиты информации.

3.2. Содержание практического блока дисциплины Очная форма обучения (полный срок)

№	Тема практического (семинарского, лабораторного) занятия
Тема 2. Экономическая информация	
ЛЗ 1	Основные понятия информационной безопасности и защиты информации
Тема 3. Информационные ресурсы предприятий и организаций	
ЛЗ 2	Стандарты информационной безопасности
ЛЗ 3	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ
Тема 4. Табличные процессоры в информационных системах	
ЛЗ 4	Инженерно-техническая защита информации
ЛЗ 5	Организационно-правовое обеспечение защиты информации
Тема 5. Базы данных в информационных системах	
ЛЗ 6	Политика информационной безопасности
ЛЗ 7	Стандарты информационной безопасности

3.3. Образовательные технологии Очная форма обучения (полный срок)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	2	3	4	5
1	Основные понятия информационной безопасности и защиты информации	Л	Дискуссия	25
2	Политика информационной безопасности	Л	Дискуссия	25
3	Стандарты информационной безопасности	ЛЗ	Дискуссия	25
4	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	Л	Мозговой штурм	25
5	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	ЛЗ	Деловая игра	100

6	Инженерно-техническая защита информации	ЛЗ	Деловая игра	100
7	Организационно-правовое обеспечение защиты информации	ЛЗ	Деловая игра	100
Итого %				31,25%

Раздел 4. Организация самостоятельной работы обучающихся

4.1. Организация самостоятельной работы обучающихся

№	Тема дисциплины	№ вопросов	№ рекомендуемой литературы
1	Основные понятия информационной безопасности и защиты информации	1 – 4	1, 2, 3
2	Политика информационной безопасности	5 – 7	1, 2, 3
3	Стандарты информационной безопасности	8 – 11	1, 2, 3, 4
4	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	12 – 13	1, 2, 5, 9
5	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	14 – 17	1, 2, 5, 9,
6	Инженерно-техническая защита информации	18 – 19	1, 2, 6, 7
7	Организационно-правовое обеспечение защиты информации	20 – 25	1, 2, 3, 6, 7, 8

Перечень вопросов, выносимых на самостоятельную работу обучающихся

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Укажите отличия санкционированного доступа к информации от несанкционированного.
4. Перечислите основные признаки классификации возможных угроз безопасности ИС
5. Дайте краткую характеристику угрозы безопасности, обозначаемой термином «троянский конь».
6. Дайте краткую характеристику угроз безопасности, обозначаемых терминами «вирус» и «червь».
7. Назовите и охарактеризуйте наиболее распространенные виды сетевых.
8. Опишите атаку «человек-в-середине». Какие средства позволяют эффективно бороться с атаками такого типа?
9. Опишите атаку типа «отказ в обслуживании» и распределенную атаку «отказ в обслуживании».
10. Опишите особенности фишинга и фарминга. Укажите меры противодействия этим атакам.
11. Каковы источники нарушений безопасности проводных корпоративных сетей?
12. Назовите основные уязвимости и угрозы беспроводных сетей.
13. Объясните понятие «политика безопасности организации».
14. Какие разделы должна содержать документально оформленная политика безопасности?
15. Какие проблемы решает верхний уровень политики безопасности?
16. Какие задачи решает средний уровень политики безопасности?
17. Каковы особенности нижнего уровня политики безопасности?
18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
19. Опишите структуру политики безопасности организации.
20. Что представляют собой специализированные политики безопасности?
21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.

22. Что представляют собой процедуры безопасности?
23. Приведите несколько примеров процедур безопасности с описанием их особенностей.
24. Перечислите основные этапы разработки политики безопасности организации.
25. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.

4.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся

Самостоятельная работа обучающихся обеспечивается следующими учебно-методическими материалами:

1. Указаниями в рабочей программе по дисциплине (п.4.1.).
2. Лекционные материалы в составе учебно-методического комплекса по дисциплине.
3. Заданиями и методическими рекомендациями по организации самостоятельной работы обучающихся в составе учебно-методического комплекса по дисциплине.
4. Глоссарием по дисциплине в составе учебно-методического комплекса по дисциплине.

Раздел 5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся

Фонд оценочных средств по дисциплине представляет собой совокупность контролирующих материалов, предназначенных для измерения уровня достижения обучающимися установленных результатов образовательной программы. ФОС по дисциплине используется при проведении оперативного контроля и промежуточной аттестации обучающихся. Требования к структуре и содержанию ФОС дисциплины регламентируются Положением о фонде оценочных материалов по программам высшего образования – программам бакалавриата, магистратуры.

5.1. Структура фонда оценочных средств Очная форма обучения (полный срок)

№	Наименование темы дисциплины	Оценочные средства			
		Л	ПЗ (ЛЗ, СЗ)	СРО	Код индикатора и дескриптора достижения компетенций
1	2	3	4	5	6
1	Основные понятия информационной безопасности и защиты информации	УО, Д	ПРВ, УО, Д	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
2	Политика информационной безопасности	УО, Д	ПРВ, УО, Д	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
3	Стандарты информационной безопасности	УО, МШ	ПРВ, УО, ДИ, ДИ	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
4	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	УО	ПРВ, УО	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
5	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	УО	ПРВ, УО, ДИ, ДИ	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
6	Инженерно-техническая защита информации	УО	ПРВ, УО, Д	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2
7	Организационно-правовое обеспечение защиты информации	УО	ПРВ, УО, Д	ПРВ	ИД-1 ОПК-6.1 ИД-2 ОПК-6.2 ИД-3 ОПК-6.1 ИД-4 ОПК-6.2 ИД-5 ОПК-6.1 ИД-6 ОПК-6.2

Условные обозначения оценочных средств (Столбцы 3, 4, 5):

ЗЗ – защита выполненных заданий (творческих, расчетных и т.д.), представление презентаций;

Т – тестирование по безмашинной технологии;

АСТ – тестирование компьютерное;

УО – устный (фронтальный, индивидуальный, комбинированный) опрос;

КР – контрольная работа (аудиторные или домашние, индивидуальные, парные или групповые контрольные, самостоятельные работы, диктанты и т.д.);

К – коллоквиум;

ПРВ – проверка рефератов, отчетов, рецензий, аннотаций, конспектов, графического материала, эссе, переводов, решений заданий, выполненных заданий в электронном виде и т.д.;

ДИ – Деловая игра;

РИ – Ролевая игра;

КМ – Кейс-метод;

КС – Круглый стол;

МШ – Метод мозгового штурма;

МКС – Метод компьютерной симуляции;

Д – Дискуссия, полемика, диспут, дебаты;

МП – Метод проектов;

ЛС – Лекция ситуация;

ЛК – Лекция-конференция;

ПЛ – Проблемная лекция;

П – Портфолио.

5.2. Оценочные средства текущего контроля

Перечень практических (семинарских) заданий

1. Какой документ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ?

А) Федеральный закон “Об информации, информационных технологиях и о защите информации”

Б) Федеральный закон “О государственной тайне”

В) Доктрина информационной безопасности Российской Федерации

Г) Стратегия национальной безопасности Российской Федерации

2. Из скольких уровней состоит правовое обеспечение информационной безопасности?

А) двух уровней

Б) трех уровней

В) четырех уровней

Г) пяти уровней

3. В структуру государственной системы защиты информации РФ входят:

А) ФСБ РФ

Б) МВД РФ

В) ФСТЭК

Г) ФСИН

4. Предметом правового регулирования в области информации, информационных технологий и защиты информации являются

А) отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации

Б) отношения, возникающие только при применении информационных технологий

В) отношения, возникающие только при обеспечении защиты информации

Г) отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации

5. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ

- А) государственная тайна
- Б) коммерческая тайна
- В) банковская тайна
- Г) конфиденциальная информация

6. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это

- А) защита информации
- Б) компьютерная безопасность
- В) защищенность информации
- Г) защищенность потребителей информации
- Д) безопасность данных

7. Преступлениям в сфере компьютерной информации в Уголовном кодексе посвящается

- А) глава
- Б) раздел
- В) статья
- Г) пункт
- Д) часть

8. Владельцем информации второй категории является...

- А) простые люди
- Б) государство
- В) коммерческая организация
- Г) муниципальное учреждение
- Д) некоммерческая организация

9. Информацией, составляющей коммерческую тайну, владеют

- А) государство
- Б) различные учреждения
- В) государственная Дума
- Г) граждане Российской Федерации
- Д) медико-социальные организации

10. О государственной тайне» был принят в следующем году

- А) 1985
- Б) 1988
- В) 1993
- Г) 2005

5.3. Перечень вопросов к итоговому контролю знаний по дисциплине

Вопросы к экзамену:

1. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов.
2. Компьютерные преступления. Основные технологии, используемые при совершении компьютерных преступлений.

3. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
4. Основные каналы утечки информации.
5. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
6. Криптография. Симметричные криптосистемы.
7. Криптография. Асимметричные криптосистемы.
8. Обзор и классификация методов шифрования информации.
9. Электронно-цифровая подпись.
10. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?
11. В чем заключаются достоинства и недостатки программных средств защиты информации?
12. Парольная защита.
13. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
14. Политика безопасности. Основные типы политики безопасности.
15. Стандарты информационной безопасности.
16. Правовое обеспечение защиты информации. Нормативные документы.
17. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.
18. Психологические аспекты информационной безопасности организации.
19. Настройка политики безопасности операционной системы.
20. Анализ защищенности изолированной программной среды.
21. Исследование систем идентификации.
22. Структура законодательной базы информационной безопасности РФ.
23. Стратегия национальной безопасности. Назначение, основные термины.
24. Доктрина ИБ. Ее назначение.
25. Структура и виды нормативных актов, регулирующих обеспечение информационной безопасности в Российской Федерации
26. Понятие о защите информации в РФ (149-ФЗ). Государственное регулирование. Обязанности обладателей информации и операторов информационных систем. Регуляторы.
27. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации

Раздел 6. Оценочные средства промежуточной аттестации (с ключами)

1. Средства защиты, призванные создать некоторую физически замкнутую среду вокруг объекта и элементов защиты замкнутую среду вокруг объекта и элементов защиты

- а) организационно-административные
- б) технические
- в) методологические
- г) программные

Правильный ответ: б)

2. Установление системы паролей относится к методу

- а) идентификации
- б) аутентификации
- в) аутентификации
- г) верификации

Правильный ответ: в)

3. Идентификация

- а) распознавание информации
- б) полное игнорирование информации
- в) присвоение какому-либо объекту или субъекту уникального имени или образа
- г) последовательность действий, приводящих к пониманию информации

Правильный ответ: в)

1. *Назначение электронной цифровой подписи:*

- а) защита данных от несанкционированного копирования
- б) удостоверение подлинности сведений
- в) выявление закономерностей построения производственных процессов
- г) ограничение доступа к информационным массивам
- д) защита программ от нелегального использования

Правильный ответ: б)

2. *Организационно-административные средства защиты*

- а) регистрация пользователей компьютерных средств в журналах
- б) разграничение доступа к информации в соответствии с функциональными обязанностями должностных лиц
- в) использование автономных средств защиты аппаратуры
- г) создание контрольно-пропускного режима на территории расположения средств обработки информации

Правильный ответ: б), г)

3. *Преимущества использования архитектуры клиент-сервер*

- а) высокое быстродействие сети
- б) низкое быстродействие сети
- в) низкая стоимость
- г) требуется большая вычислительная мощность от сервера
- д) требуется небольшая вычислительная мощность от ПК

Правильный ответ: а), д)

4. *Методы, которые относятся к криптографическим преобразованиям*

- а) замена
- б) идентификация
- в) установка электронной цифровой подписи
- г) перестановка

Правильный ответ: а), г)

5. *Существующие средства защиты информации*

- а) технические
- б) технологические
- в) организационно-административные
- г) модифицирующие
- д) программные

Правильный ответ: а), б), в) д)

6. *Сложный пароль*

- а) состоит из более 8 символов
- б) состоит из более 3 символов
- в) включает только английские буквы
- г) включает только русские буквы
- д) не является определенным словом

Правильный ответ: а), д)

7. *Способность системы выполнять требуемую работу в течение заданного времени*

Правильный ответ: надежность

8. Пользователь, который имеет полный набор прав доступа для всего компьютера и неограниченный доступ ко всем файлам и ключам системного реестра называется _____

Правильный ответ: администратор

9. Средства защиты, призванные создать некоторую физически замкнутую среду вокруг объекта и элементов защиты замкнутую среду вокруг объекта и элементов защиты, называются _____

Правильный ответ: технические

10. Присвоение какому-либо объекту или субъекту уникального имени или образа _____

Правильный ответ: идентификация

11. Установление подлинности объекту или субъекту _____

Правильный ответ: аутентификация

12. Защита данных методом их шифрования _____

Правильный ответ: криптография

13. Компьютерный вирус _____

Правильный ответ: программа, способная самопроизвольно создавать свои копии и выполнять несанкционированные действия

14. Криптография _____

Правильный ответ: защита данных методом шифрования

15. Надежность _____

Правильный ответ: способность системы выполнять требуемую работу в течение заданного времени

16. Безопасность информации _____

Правильный ответ: способность системы обеспечить защиту информации от негативных явлений

17. При симметричном методе шифрования _____

Правильный ответ: шифрование и расшифровка документа осуществляется одним ключом

18. Идентификация _____

Правильный ответ: присвоение субъекту или объекту уникального имени

19. Установите соответствие

1) идентификация	а) присвоение какому-либо объекту или субъекту уникального имени или образа
2) аутентификация	б) установление подлинности
3) система защиты информации	в) совокупность организационных и технологических мер, технических средств, правовых норм, направленных на противодействие угрозам нарушителей

Правильный ответ:

1) – а)

2) – б)

3) – в)

Раздел 7. Перечень учебной литературы, необходимой для освоения дисциплины

7.1. Основная литература

1. Медведев, В. А., Информационная безопасность. Введение в специальность + Приложение: Тесты : учебник / В. А. Медведев. - Москва : КноРус, 2023. - 143 с. - ISBN 978-5-406-11334-9. - URL: <https://book.ru/book/948870>. - Текст : электронный.
2. Мельников, В. И., Информационная безопасность : учебник / В. И. Мельников, А. И. Куприянов, Т. Ю. Васильева. - Москва : КноРус, 2023. - 371 с. - ISBN 978 5-406-11960-0. - URL: <https://book.ru/book/950148>. - Текст : электронный.
3. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - Москва : РИОР : ИНФРА-М, 2021. - 400 с. - URL: <http://new.ibooks.ru/bookshelf/361250>. - Текст : электронный.

7.2. Дополнительная литература

1. Крылов, Г. О., Базовые понятия информационной безопасности : учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. - Москва : Русайнс, 2023. - 257 с. - ISBN 978-5-466-01996-4. - URL: <https://book.ru/book/946979>. - Текст : электронный.
2. Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. - Москва : КноРус, 2022. - 189 с. - ISBN 978-5-406-08880-7. - URL: <https://book.ru/book/941751>. - Текст : электронный.
3. Организационно-правовое обеспечение информационной безопасности : учебное пособие для вузов / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.]; под ред. А. А. Стрельцова. - М.: Академия, 2008. - 256 с. - ISBN 978-5-7695-4240-4. - Текст : непосредственный.
4. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А.А. Малюк. - М.: Горячая линия - Телеком, 2004. - 280 с. - Текст : непосредственный.

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. <http://elibrary.ru/>
2. <https://habr.com/>
3. Справочно-правовая система «Консультант Плюс».
4. «Гарант»
5. ПО для организации конференций

Раздел 8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

8.1. Учебные аудитории для проведения лекционных и практических занятий (для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации обучающихся всех направлений подготовки).

Учебная компьютерная аудитория оборудована:

- Стол для преподавателя
 - Стул для преподавателя
 - Столы для обучающихся
 - Стулья для обучающихся
 - Моноблок для преподавателя с выходом в интернет
 - ЖК панель
 - Компьютеры для обучающихся
 - комплект учебно-наглядных пособий по дисциплине
- Программные средства для проведения практических занятий:
- nanoCAD2025 на 20 посадочных мест.

8.2. Помещение для самостоятельной работы обучающихся (помещение общего пользования с подключением к системам телекоммуникации и с обеспечением доступа в электронную информационно-образовательную среду (доступ в сеть Интернет, Wi-Fi, глобальные поисковые системы, электронная почта и т.д.)

Специализированная мебель и технические средства обучения:

- Стол для преподавателя
- Стул для преподавателя
- Столы для обучающихся
- Стулья для обучающихся
- Компьютеры для преподавателя с выходом в интернет
- Компьютеры для обучающихся выходом в интернет
- ПО: MS Office, Яндекс браузер
- Цифровой образовательный ресурс IPR SMART
- доступ в ЭИОС.

Раздел 9. Методические указания для обучающихся по освоению дисциплины

Для успешного усвоения материала курса требуются значительное время, концентрация внимания и усилия: посещение лекционных занятий и конспектирование преподаваемого материала, работа с ним дома, самостоятельная проработка материала рекомендуемых учебников и учебных пособий при самостоятельной подготовке. Особое внимание следует обратить на выполнение практических работ, практических заданий по СРО, тестовых вопросов.

При самостоятельной работе с учебниками и учебными пособиями полезно иметь под рукой справочную литературу (энциклопедии) или доступ к сети Интернет, так как могут встречаться новые термины, понятия, которые раньше обучающиеся не знали.

Цель практических занятий по дисциплине - закрепление знаний по определенной теме, приобретенных в результате прослушивания лекций, получения консультаций и самостоятельного изучения различных источников литературы. При выполнении данных работ обучающиеся должны будут глубоко изучить состав и принцип работы современных информационных систем. Получить практические навыки работы с современными ИС.

Перед практическим занятием обучающийся должен детально изучить теоретические материалы вопросов практики в учебниках, конспектах лекций, периодических журналах и прочее. Если при выполнении практического задания у обучающегося остаются неясности, то ему необходимо оперативно обратиться к преподавателю за уточнением.

После выполнения практического задания обучающиеся должны выполнить самостоятельную работу. Самостоятельная работа включает в себя индивидуальное задание по пройденной теме. Таким образом, каждый обучающийся выполняет только свой вариант задания.

При дистанционном выполнении практических работ обучающийся может самостоятельно приобрести операционные системы Windows XP, Windows 7, Windows 8, Windows 10 и пакет MicrosoftOffice(OpenOffice). Также обучающийся может скачать с официального сайта 1С учебную версию программы 1С:Предприятие. Ответственность за установку и настройку программного обеспечения в данном случае ложится на обучающегося. Следует воспользоваться методическими указаниями по установке данных программных систем.

Результаты выполненных заданий оцениваются с учетом теоретических знаний по соответствующим разделам дисциплины, техники выполнения работы, объективности и обоснованности принимаемых решений в процессе работы с данными, качества оформления. Переход к выполнению следующего практического задания допускается только после отчета выполненной работы.

Учебно-методическое издание

Рабочая программа учебной дисциплины

Основы информационной безопасности

(Наименование дисциплины в соответствии с учебным планом)

Филиппов Михаил Владимирович

(Фамилия, Имя, Отчество составителя)
