

УТВЕРЖДАЮ
Декан факультета

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	И Робототехника и инновационная инженерия
Выпускающая кафедра	И2 Программная инженерия и интеллектуальные системы
Кафедра-разработчик рабочей программы	И2 Программная инженерия и интеллектуальные системы

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	
1	1	3	108	17	17	0	0	91	0	0	91	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: 2026

Программу составили:

Кафедра Н2 Программная инженерия и интеллектуальные системы
Палехова Ольга Александровна, старший преподаватель

Кафедра Н2 Программная инженерия и интеллектуальные системы
Наурусова Гульнара Ахмановна, старший преподаватель

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **Н2 Программная инженерия и интеллектуальные системы**

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

Программа рассмотрена
на заседании выпускающей кафедры

Н2 Программная инженерия и интеллектуальные системы

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

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:

УК-6 — Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

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

Формированию компетенций служит достижение следующих результатов образования:

УК-6

знания:

особенностей подготовки специалиста в области информационной безопасности, требований к самоорганизации и профессиональному росту;

правил внутреннего распорядка и Устава университета;;

умения:

самостоятельно находить и отбирать необходимый теоретический материал, связанный с выбранным направлением;

ориентироваться в учебном плане направления;

ОПК-3

знания:

основные понятия и принципы информационной безопасности (конфиденциальность, целостность, доступность);

классификация угроз и уязвимостей;

нормативно-правовая база в области защиты информации (федеральные законы, ГОСТ);

основы криптографической защиты, методы и средства обеспечения ИБ;;

умения:

применять стандарты и нормативные документы для решения типовых задач защиты информации;

оформлять отчетную документацию в соответствии с ГОСТ 7.32-2017 и стандартами по защите информации;

самостоятельно находить и отбирать необходимый теоретический материал, связанный с выбранным направлением;;

навыки:

работы с профессиональными источниками информации (базы данных уязвимостей, нормативно-справочные системы);

уверенное использование ИКТ с соблюдением требований информационной безопасности;

оформления отчетной документации в соответствии с ГОСТ 7.32-2017 "Отчет о научно-исследовательской работе"..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением содержания школьных курсов и служит основой для освоения дисциплин: **ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ, СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ, ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Требования к уровню подготовки обучающихся и предварительные компетенции определены Федеральным государственным образовательным стандартом среднего общего образования.

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		УК-6	ОПК-3
1	1	Раздел 1. Организация учебного процесса в БГТУ "Военмех". 1.1. Устав Университета, правила внутреннего распорядка. 1.2. Органы управления БГТУ, структура университета, организация учебного процесса. 1.3. Права и обязанности обучающегося. 1.4. Знакомство с сайтом БГТУ, поиск информации. 1.5. Балльно-рейтинговая система БГТУ "Военмех", положение о текущем контроле успеваемости и промежуточной аттестации обучающихся.	14	4	4	10	0	0
1	1	Раздел 2. Направление 09.03.02 и профиль подготовки бакалавров. 2.1. IT-сфера. Варианты построения карьеры в IT-отрасли. 2.2. ФГОС ВО бакалавриата по направлению подготовки 09.03.02 Информационные системы и технологии 2.3 Профессиональные стандарты 06.001 Программист, 06.030 - Специалист по защите информации в телекоммуникационных системах и сетях, 06.004 Специалист по тестированию в области информационных технологий. Обобщенные трудовые функции и компетенции. 2.4. Обзор учебного плана БГТУ по направлению.	14	4	4	10	10	20
1	1	Раздел 3. Основы информационной безопасности. 3.1. Базовые понятия: конфиденциальность, целостность, доступность. 3.2. Угрозы информационной безопасности: классификация, источники, примеры. 3.3. Уязвимости компьютерных систем и способы их эксплуатации. 3.4. Модель нарушителя и классификация атак. 3.5. Построение политики информационной безопасности организации.	22	2	2	20	20	10
1	1	Раздел 4. Правовые и организационные основы информационной безопасности. 4.1. Федеральный закон «Об информации, информационных технологиях и о защите информации». 4.2. Закон «О персональных данных». 4.3. Доктрина информационной безопасности Российской Федерации. 4.4. Организационные меры защиты: регламенты, инструкции, категорирование объектов. 4.5. Обзор стандартов ГОСТ Р ИСО/МЭК 2700 ГОСТ 34-й серии и Единой системы программной документации применительно к защищенным системам.	25	2	2	23	35	30
1	1	Раздел 5. Оформление технической документации. 5.1. ГОСТ 7.32-2017 "Отчет о научно-исследовательской работе". 5.2. ГОСТ 19.х Единая система программной документации (ЕСПД). 5.3. ГОСТ 34.х Информационные технологии. Комплекс стандартов на автоматизированные системы.	9	2	2	7	0	10
1	1	Раздел 6. Технические и программные средства защиты информации. 5.1. Методы идентификации и аутентификации; управление доступом. 5.2. Межсетевые экраны, системы обнаружения и предотвращения вторжений. 5.3. Антивирусная защита и защита от вредоносного ПО. 5.4. Средства защиты от утечек информации. 5.5. Основы построения защищенных информационных систем.	24	3	3	21	35	30
Всего за 1 семестр			108	17	17	91	100	100
Всего по дисциплине			108	17	17	91	100	100

3.2. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Организация учебного процесса в БГТУ "Военмех".	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	9
2		Выполнение части творческого задания	1
3	Раздел 2. Направление 09.03.02 и профиль подготовки бакалавров.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	9
4		Выполнение части творческого задания	1
5	Раздел 3. Основы информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	9
6		Выполнение части творческого задания	1
7		Сбор материала для реферата	10
8	Раздел 4. Правовые и организационные основы информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	12
9		Выполнение части творческого задания	1
10		Анализ собранного материала и написание реферата	10
11	Раздел 5. Оформление технической документации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
12		Оформление реферата	3
13	Раздел 6. Технические и программные средства защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	20
14		Выполнение части творческого задания	1
Всего за 1 семестр			91

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
1						ДР			Тв.зад	ДР					Реф	ДР	зач.

Условные обозначения:

- ДР – диагностическая работа;
- Тв.зад – творческое задание;
- Реф – реферат;
- зач. – зачет.

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

- диагностическая работа;
- творческое задание;
- реферат.

Промежуточная аттестация проводится в формах:

- зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. . Образовательное право. Москва: Юрайт, 2021, эл. рес.
2. . Отчёт о научно-исследовательской работе. Структура и правила оформления. М.: Стандартинформ, 2017, эл. рес.
3. Б. Я. Советов, В. В. Цехановский. . Информационные технологии. Москва: Юрайт, 2022, эл. рес.
4. В. К. Волк. . Практическое введение в программную инженерию. Санкт-Петербург: Лань, 2022, эл. рес.
5. Е. М. Лаврищева. . Программная инженерия. Парадигмы, технологии и CASE-средства. Москва: Юрайт, 2023, эл. рес.
6. С. В. Веретехина, В. В. Веретехин. . Информационные технологии. Пакеты программного обеспечения общего блока "IT-инструментарий". М.: Русайнс, 2017, 30 экз.
7. С. Макконнелл. Совершенный код. М.: Русская Редакция, 2005, эл. рес.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

1. Прикладная информатика.

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

1. <https://www.voenmeh.ru/> - сайт БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова;
2. https://www.voenmeh.ru/images/docs/Ustav_16_11_2018.pdf - Устав БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова;
3. https://www.voenmeh.ru/images/docs/PRIKAZ_38_O_ot_30_01_2023_Ob_utverzhenii_pravil_vnutrennego_rasporyadka_ECP.pdf - Правила внутреннего распорядка;
4. https://www.voenmeh.ru/images/docs/uch_upr/Prikaz_ot_16_09_2022_698_izm_v3.pdf - Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся;
5. https://www.voenmeh.ru/images/docs/otdel-trudoustroystva/Prikaz_534_o_Polojenie_o_practic_podgotovke_2023_v1.pdf - Положение о практической подготовке обучающихся;
6. <http://library.voenmeh.ru/jirbis2> - Библиотечно-издательский центр БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
7. <https://urait.ru/> - Образовательная платформа Юрайт. Для вузов и ссузов.;
8. <http://e.lanbook.com/> - ЭБС Лань;
9. https://fgosvo.ru/uploadfiles/FGOS%20VO%203++/Bak/090304_B_3_15062021.pdf - ФГОС ВО бакалавриата по направлению подготовки 09.03.04 Программная инженерия;
10. <https://mintrud.gov.ru/docs/mintrud/orders/2403> - Профессиональный стандарт 06.001 Программист;
11. <https://mintrud.gov.ru/docs/mintrud/orders/1649> - Профессиональный стандарт 06.028 Системный программист;
12. <https://mintrud.gov.ru/docs/mintrud/orders/2638> - Профессиональный стандарт 06.022 Системный аналитик;
13. <https://mintrud.gov.ru/docs/mintrud/orders/2083> - профессиональный стандарт 06.004 Специалист по тестированию в области информационных технологий;
14. <https://fgos.ru/fgos/fgos-09-03-02-informacionnye-sistemy-i-tehnologii-219/> - ФГОС 09.03.02 Информационные системы и технологии;
15. <https://mintrud.gov.ru/docs/mintrud/orders/2446> - Приказ Минтруда России № 525н от 14 сентября 2022 г.;
16. Шаньгин, В. Ф. 2. Информационная безопасность компьютерных систем и сетей : [Электронный ресурс] : учебное пособие / Шаньгин В. Ф. - М. : ФОРУМ ; М. : ИНФРА-М, 2021. - 416 с. - URL: <http://ibooks.ru/reading.php?productid=361273>. - ISBN 978-5-8199-0754-2 : Б. ц.;
17. <https://docs.cntd.ru/document/1200181803> - ГОСТ 34.201-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.;
18. <https://docs.cntd.ru/document/1200007627> - ГОСТ 19.101-77 Единая система программной документации. Виды программ и программных документов..

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
3. <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:

не требуется.

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. 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 **ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *Н Робототехника и инновационная инженерия* БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой *Н2 Программная инженерия и интеллектуальные системы*.

Дисциплина нацелена на формирование *компетенций*:

УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;

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.

Содержание дисциплины охватывает круг вопросов, связанных с анализом профессиональных задач, для решения которых проводится подготовка по данному направлению и профилю, особенностей подготовки на кафедре и факультете, обусловленных потребностями предприятий и организаций – партнеров БГТУ, структурой направления и профстандарты в области ИБ; основами информационной безопасности (угрозы, уязвимости, политика безопасности); правовым и организационным обеспечением; техническими и криптографическими методами защиты информации.

Программой дисциплины предусмотрены следующие **виды контроля**:

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

- диагностическая работа;
- творческое задание;
- реферат.

Промежуточная аттестация проводится в формах:

- зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены лекционные занятия (**17 ч.**), самостоятельная работа студента (**91 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 17 ч. аудиторных занятий, и 91 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. Организация учебного процесса в БГТУ "Военмех".		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	. Образовательное право: Москва: Юрайт, 2021 (4, 5, 8, 9)	9
Выполнение части творческого задания		1
Итого по разделу 1		10
Раздел 2. Направление 09.03.02 и профиль подготовки бакалавров.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	. Образовательное право: Москва: Юрайт, 2021 (4)	9
Выполнение части творческого задания		1
Итого по разделу 2		10
Раздел 3. Основы информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. В. Веретехина, В. В. Веретехин. . Информационные технологии. Пакеты программного обеспечения общего блока "IT-инструментарий": М.: Русайнс, 2017 (1-3) Б. Я. Советов, В. В. Цехановский. . Информационные технологии: Москва: Юрайт, 2022 (1-4)	9
Выполнение части творческого задания		1
Сбор материала для реферата		10
Итого по разделу 3		20
Раздел 4. Правовые и организационные основы информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. К. Волк. . Практическое введение в программную инженерию: Санкт-Петербург: Лань, 2022 (1, 2)	12
Выполнение части творческого задания		1
Анализ собранного материала и написание реферата		10
Итого по разделу 4		23
Раздел 5. Оформление технической документации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	. Отчёт о научно-исследовательской работе. Структура и правила оформления: М.: Стандартинформ, 2017 (полностью)	4
Оформление реферата		3
Итого по разделу 5		7
Раздел 6. Технические и программные средства защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. Макконнелл. Совершенный код: М.: Русская Редакция, 2005 (1-7) Е. М. Лаврищева. . Программная инженерия. Парадигмы, технологии и CASE-средства: Москва: Юрайт, 2023 (2)	20
Выполнение части творческого задания		1
Итого по разделу 6		21

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- творческое задание;
- реферат;
- 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.

Творческое задание

Творческое задание "Составление словаря IT-терминов, понятий, названий профессий и просто жаргонных словечек, используемых в сфере информационных технологий в целом и в программной инженерии в частности". Работа выполняется совместно всеми студентами первого курса кафедры О7.

За каждое новое добавленное слово дается до 3 баллов, за добавленное определение уже имеющегося в словаре слова до 2 баллов в зависимости от правильности данного определения.

Количество добавленных слов может быть любым, сумма баллов не может превышать 14.

Реферат

Темы рефератов

1. Информационная безопасность: основные понятия и актуальность.
2. История развития криптографии.
3. Угрозы информационной безопасности в современных компьютерных системах.
4. Модель нарушителя и классификация атак.
5. Каналы утечки информации и меры противодействия.
6. Правовое регулирование защиты информации в Российской Федерации.
7. Федеральный закон «Об информации, информационных технологиях и о защите информации»: основные положения.
8. Способы защиты персональных данных.
9. Доктрина информационной безопасности РФ.
10. Организационные меры обеспечения информационной безопасности на промышленном предприятии.
11. Управление рисками информационной безопасности.
12. Стандарты в области информационной безопасности (ISO/IEC 27001, ГОСТ Р ИСО/МЭК).
13. Методы аутентификации пользователей.
14. Управление доступом в компьютерных системах.
15. Межсетевые экраны: принципы работы и эволюция.
16. Системы обнаружения и предотвращения вторжений.
17. Вредоносное программное обеспечение: классификация, способы распространения и методы защиты.
18. Антивирусная защита корпоративных сетей.
19. DLP-системы: предотвращение утечек конфиденциальной информации.
20. Криптографические методы защиты информации.
21. Симметричное и асимметричное шифрование.
22. Электронная цифровая подпись: принципы, применение, юридическая сила.
23. Инфраструктура открытых ключей и удостоверяющие центры.
24. Хэш-функции и их роль в информационной безопасности.
25. Защита информации в беспроводных сетях.
26. Безопасность облачных технологий и сервисов.
27. Защита информации в мобильных устройствах и платформах.
28. Социальная инженерия: методы атак и способы противодействия.
29. Интернет вещей (IoT) и проблемы безопасности.
30. Безопасность автоматизированных систем управления технологическими процессами (АСУ ТП).
31. Методы защиты критической информационной инфраструктуры.
32. Компьютерная разведка и техники сбора информации об объекте атаки.
33. Анализ защищенности и аудит информационной безопасности.
34. Системы менеджмента информационной безопасности.
35. Восстановление после инцидентов кибератак.
36. Квантовая криптография и перспективы постквантовых алгоритмов.
37. Безопасность электронной почты.
38. Безопасность веб-приложений.
39. Цифровой след в сети Интернете.
40. Нормативная база ФСТЭК России по защите информации.
41. Категорирование объектов информатизации и защита государственной тайны.

Требования к реферату

1. Объем не менее 10 страниц.
2. Количество используемых источников (в т.ч. интернет-ресурсов) - не менее 5, обязательно должны быть использованы источники, опубликованные в последние 5 лет.

3. Оформление в соответствии с ГОСТ 7.32-2017 "Отчет о научно-исследовательской работе".

Критерии и подробный рубрикатор оценивания приведены в технологической карте и на странице курса в ЭИОС moodle.voenmeh.ru

Зачет

Для получения зачёта студенту необходимо ответить на 2 вопроса преподавателя, при ответе допускаются неточности, недостаточно правильные формулировки, однако ответы должны быть даны по существу вопроса. Вопросы приведены в УМК дисциплины.

В соответствии с БРС итоговая оценка "зачтено" выставляется при наборе обучающимся 60 и более баллов. Порядок начисления баллов прописан в технологической карте.

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме		Самостоятельная работа студентов	Формируемая компетенция, %		НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции		УК-6	ОПК-3	
1	1	Раздел 1. Организация учебного процесса в БГТУ "Военмех".	14	4	4	10	0	0	Творческое задание
1	1	Раздел 2. Направление 09.03.02 и профиль подготовки бакалавров.	14	4	4	10	10	20	Творческое задание
1	1	Раздел 3. Основы информационной безопасности.	22	2	2	20	20	10	Реферат, Творческое задание
1	1	Раздел 4. Правовые и организационные основы информационной безопасности.	25	2	2	23	35	30	Реферат, Творческое задание
1	1	Раздел 5. Оформление технической документации.	9	2	2	7	0	10	Реферат
1	1	Раздел 6. Технические и программные средства защиты информации.	24	3	3	21	35	30	Творческое задание, Реферат
Всего за 1 семестр			108	17	17	91	100	100	
Всего по дисциплине			108	17	17	91	100	100	

Оценочные материалы по дисциплине ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

УК-6 - Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

- № 1 Прочитайте текст и запишите развернутый обоснованный ответ
Ядром любой информационной системы является _____ под управлением _____.
- № 2 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие признаки из перечисленных указывают на необходимость рефакторинга?
1. в тексте программы присутствуют трудночитаемые идентификаторы
 2. в тексте программы присутствуют глобальные константные переменные
 3. одной из функций в программе передается более 10 аргументов
 4. в некоторых функциях присутствует больше одного оператора return
 5. в тексте программы есть повторяющиеся фрагменты
- № 3 Прочитайте текст и установите последовательность
Расположите в правильной последовательности основные этапы составления и выполнения программы на компьютере.
1. Выполнение программы
 2. Компиляция и компоновка программы
 3. Написание программы
 4. Оценка результатов
 5. Постановка задачи
 6. Построение алгоритма
- № 4 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой нормативный документ устанавливает правовые, организационные и экономические основы образования в Российской Федерации, основные принципы государственной политики Российской Федерации в сфере образования, общие правила функционирования системы образования и осуществления образовательной деятельности, определяет правовое положение участников отношений в сфере образования?
1. Федеральный закон №273-ФЗ «Об образовании в Российской Федерации»
 2. Федеральный государственный образовательный стандарт высшего образования
 3. Устав образовательной организации
 4. Положение о Министерстве науки и высшего образования Российской Федерации
- № 5 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Что является ключевым принципом управления своей образовательной траекторией для будущего специалиста по информационной безопасности?
1. Достаточно одного полученного диплома на всю жизнь
 2. Необходимо постоянное обновление знаний и навыков в соответствии с меняющимся ландшафтом угроз
 3. Достаточно каждые пять лет полностью менять сферу деятельности
 4. Главное – использовать только самые новые программные продукты, не изучая базовые принципы
- № 6 Прочитайте текст и установите последовательность
Установите соответствие между нормативным документом и его содержанием.
1. ГОСТ 7.32-2017
 2. ГОСТ Р ИСО/МЭК 27001
 3. Устав БГТУ «ВОЕНМЕХ»
- А. Устанавливает требования к системе менеджмента информационной безопасности
Б. Регламентирует структуру, правила оформления отчёта о научно-исследовательской работе
В. Закрепляет права, обязанности обучающихся и общие нормы организации учебного процесса
- № 7 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какой федеральный орган исполнительной власти осуществляет контроль и надзор в области технической защиты информации конфиденциального характера (за исключением криптографических средств)?
1. ФСБ России
 2. ФСТЭК России
 3. Роскомнадзор
 4. Минцифры России
- № 8 Прочитайте текст и установите соответствие
Установите соответствие между профессиональными стандартами и обобщёнными трудовыми функциями.
1. Специалист по защите информации
 2. Специалист по технической защите конфиденциальной информации
- А. Проведение работ по комплексной защите информации
Б. Разработка и внедрение системы обеспечения информационной безопасности
Г. Проверка защищенности информации

- № 9 Прочитайте текст и запишите развернутый обоснованный ответ
Что такое политика информационной безопасности организации?
- № 10 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Отметьте обобщенные трудовые функции программиста, указанные в соответствующем профессиональном стандарте.
1. Обеспечение функционирования баз данных
 2. Руководство разработкой технической документации продукта
 3. Разработка и отладка программного кода
 4. Проверка работоспособности и рефакторинг кода программного обеспечения

- № 11 Прочитайте текст и установите соответствие
Установите соответствие типов ЭВМ и их особенностей. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца.

Тип ЭВМ	Особенности
1. ЦВМ	А. Состоит из аналоговой и цифровой частей
2. АВМ	Б. Электромеханические элементы
3. Гибридная вычислительная система	В. Выполнение вычислений в непрерывном времени
	Г. Дискретизация обрабатываемых сигналов по времени и по уровню

- № 12 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой Федеральный закон регулирует защиту персональных данных в Российской Федерации?

1. Федеральный закон «Об информации, информационных технологиях и о защите информации»
2. Федеральный закон «О персональных данных»
3. Федеральный закон «О безопасности критической информационной инфраструктуры РФ»
4. Федеральный закон «О государственной тайне»

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, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой криптографический алгоритм лежит в основе создания электронной цифровой подписи, использующей асимметричное преобразование?

1. AES
2. SHA-256
3. RSA
4. MD5

- № 2 Прочитайте текст и установите соответствие
Установите соответствие между средством защиты информации и его типом.

1. Шифрование жёсткого диска с помощью алгоритма AES
 2. Инструкция по парольной политике организации
 3. Источник бесперебойного питания и система резервного копирования
- А. Криптографическая мера защиты
Б. Программно-техническая мера защиты (обеспечение доступности)
В. Организационная мера защиты
Г. Правовая мера защиты

- № 3 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Отметьте критерии оценки надежности программного обеспечения.

1. Отказоустойчивость
2. Завершенность
3. Отслеживаемость
4. Восстанавливаемость
5. Функциональная полнота

- № 4 Прочитайте текст и запишите развернутый обоснованный ответ
Что такое социальная инженерия? Приведите реальный пример фишинговой атаки и объясните, как пользователь может её распознать.

- № 5 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Самый длительный этап в жизненном цикле программного обеспечения – это...

1. изучение предметной области
 2. программирование
 3. тестирование
 4. эксплуатация
- № 6 Прочитайте текст и запишите развернутый обоснованный ответ
Дайте определение понятию «угроза информационной безопасности». Какими источниками могут создаваться угрозы?
- № 7 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие характеристики определяют функциональную пригодность программного обеспечения? Отметьте все верные варианты ответа.
1. Функциональная целесообразность
 2. Функциональная грамотность
 3. Функциональная корректность
 4. Функциональная полнота
 5. Функциональная анализируемость
- № 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какая из перечисленных уязвимостей позволяет злоумышленнику выполнить произвольные SQL-запросы к базе данных через веб-приложение?
1. Межсайтовый скриптинг (XSS)
 2. Межсайтовая подделка запроса (CSRF)
 3. SQL-инъекция
 4. Переполнение буфера
- № 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие из перечисленных действий относятся к лучшим практикам обеспечения информационной безопасности на рабочем месте? (Выберите все правильные варианты.)
1. Регулярная установка обновлений безопасности операционной системы и прикладного ПО
 2. Использование сложных уникальных паролей и двухфакторной аутентификации
 3. Отключение антивирусного сканера для ускорения запуска незнакомых файлов
 4. Создание резервных копий важных данных на отключённом от сети носителе
 5. Отправка конфиденциальных документов через общедоступные мессенджеры без шифрования
- № 10 Прочитайте текст и установите соответствие
Сопоставьте термины и определения, которые им соответствуют.
1. Конфиденциальность
 2. Целостность
 3. Доступность
- А. Защищённость информации от неправомерного ознакомления, раскрытия третьим лицам
Б. Свойство информации быть полученной авторизованным пользователем в требуемое время без необоснованных задержек
В. Гарантия того, что данные не были изменены или уничтожены неправомерным или случайным образом
Г. Понятность и непротиворечивость информации
- № 11 Прочитайте текст и установите последовательность
Упорядочьте шаги базового процесса управления инцидентами информационной безопасности (от момента возникновения до анализа).
1. Обнаружение события (инцидента)
 2. Идентификация и первичная классификация инцидента
 3. Локализация и сдерживание последствий
 4. Расследование и сбор доказательств
 5. Восстановление работоспособности систем
 6. Анализ причин и совершенствование мер защиты
- № 12 Прочитайте текст и установите последовательность
Расположите действия при обнаружении инцидента информационной безопасности в правильном порядке:
1. Устранение инцидента.
 2. Анализ причин инцидента.
 3. Обнаружение и классификация инцидента.