

УТВЕРЖДАЮ
 Декан факультета

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ 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	Н Робототехника и инновационная инженерия
Выпускающая кафедра	Н2 Программная инженерия и интеллектуальные системы
Кафедра-разработчик рабочей программы	Н2 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	
3	5	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: 2026

Программу составил:

Кафедра Н2 Программная инженерия и интеллектуальные системы
Кузьмич Александр Александрович, к.т.н., доцент, доцент

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 ОСНОВЫ 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:

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

ПК-2.2 — Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Формированию компетенций служит достижение следующих результатов образования:

ПК-2.1

знания:

основные понятия информационной безопасности, защиты информации, угроз, уязвимостей, рисков и инцидентов информационной безопасности;

назначение стандартов, нормативных и методических документов в области информационной безопасности, применяемых при оценке защищённости информационных систем;

умения:

проводить базовый анализ защищённости информационной системы, выявлять значимые информационные активы, угрозы, уязвимости и риски, а также оценивать работу отдельных защитных механизмов в рамках учебного кейса;

навыки:

выполнять инструментальную проверку отдельных защитных механизмов на учебном изолированном стенде и оформлять результаты проверки в виде отчёта.

ПК-2.2

знания:

виды защищаемой информации, информационные активы, основные свойства защищаемой информации, включая конфиденциальность, целостность и доступность, а также типовые угрозы безопасности информации;

подходы к моделированию угроз, оценке рисков и выбору базовых мер защиты информационных систем;

умения:

определять информационные ресурсы и информационные активы, подлежащие защите, устанавливать возможные угрозы и оценивать риски их реализации для типовой информационной системы;

навыки:

составлять карту рисков информационной безопасности и обосновывать выбор организационных и технических мер защиты информации;

формировать краткое аналитическое заключение по результатам рассмотрения учебного кейса информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ 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: **ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ, СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.**

Содержание дисциплины является основой для освоения дисциплин: **АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ.**

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-2 — Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
- ОПК-3 — Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ОПК-5 — Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем
- ОПК-6 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий
- ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем
- ПК-93 — Способен генерировать новые идеи для решения задач цифровой экономики, абстрагироваться от стандартных моделей, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов
- 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

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		ПК-2.1	ПК-2.2
3	5	Раздел 1. Организационно-правовые основы и угрозы. 1.1. Доктрина информационной безопасности Российской Федерации и правовые основы защиты информации 1.2. Стандарты и методологии оценки рисков информационной безопасности.	24	8	4	4	16	20	40
3	5	Раздел 2. Техническая защита информации. 2.1. Криптографические методы защиты 2.2. Защита операционных систем и СУБД.	21	7	4	3	14	25	20
3	5	Раздел 3. Безопасность приложений и сетей. 3.1. Сетевая безопасность и защита периметра информационной системы 3.2. Сканирование сетей и проверка эффективности механизмов фильтрации 3.3. Безопасная разработка веб-приложений и основы DevSecOps.	40	12	6	6	28	35	25
3	5	Раздел 4. Реагирование на инциденты и итоговый практический кейс. 4.1. Киберустойчивость, мониторинг и реагирование на инциденты информационной безопасности 4.2. Обобщение результатов изучения дисциплины и подготовка к итоговому практическому кейсу.	23	7	3	4	16	20	15
Всего за 5 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. Организационно- правовые основы и угрозы.	Анализ информационных активов и моделирование угроз для выбранного объекта защиты	2
2		Оценка рисков информационной безопасности на основе упрощённой учебной модели с учётом подходов ФСТЭК России	2
3	Раздел 2. Техническая защита информации.	Настройка защищённого сетевого соединения	1
4		Харденинг сервера и защита баз данных	2
5	Раздел 3. Безопасность приложений и сетей.	Настройка правил межсетевого экранирования, регистрация сетевых событий и проверка механизмов фильтрации	4
6		Поиск признаков типовых уязвимостей веб- приложений	2
7	Раздел 4. Реагирование на инциденты и итоговый практический кейс.	Рассмотрение признаков инцидента информационной безопасности по журналам событий	2
8		Итоговая защита практического кейса	2
Всего за 5 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Организационно-правовые основы и угрозы.	Изучение нормативно-правовых основ информационной безопасности и требований к защите информации	6
2		Изучение подходов к идентификации информационных активов, моделированию угроз и оценке рисков	10
3	Раздел 2. Техническая защита информации.	Изучение основ криптографической защиты информации и защищённых сетевых соединений	6
4		Изучение вопросов защиты операционных систем, баз данных и безопасного администрирования серверов	8
5	Раздел 3. Безопасность	Изучение принципов сетевой безопасности, межсетевого	6

	приложений и сетей.	экранирования, IDS/IPS и защиты периметра информационной системы	
6		Изучение методов сканирования сетей и проверки эффективности механизмов фильтрации в учебной среде	10
7		Изучение основ безопасной разработки веб-приложений, типовых уязвимостей и подходов DevSecOps	8
8		Обобщение результатов практических работ по сетевой безопасности и безопасности веб-приложений	4
9	Раздел 4. Реагирование на инциденты и итоговый практический кейс.	Изучение основ мониторинга событий безопасности, киберустойчивости и реагирования на инциденты информационной безопасности	8
10		Обобщение подходов к защите информационных систем и подготовка к итоговому практическому кейсу	4
11		Подготовка материалов для защиты итогового практического кейса	4
Всего за 5 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
5			Отч. по ПЗ		Отч. по ПЗ	ДР	Отч. по ПЗ		Отч. по ПЗ	ДР		Отч. по ПЗ		Отч. по ПЗ	Отч. по ПЗ, Вопр.Диф.Зач	ДР	Отч. по ПЗ, диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр.Диф.Зач – вопросы к дифференцированному зачету;
- диф. зач. – дифференцированный зачет.

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

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к дифференцированному зачету.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. А. Бирюков. . Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2017, эл. рес.
2. Е. В. Глинская, Н. В. Чичварин. . Информационная безопасность конструкций ЭВМ и систем. Москва: ИНФРА-М, 2021, эл. рес.
3. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.
4. Э. Таненбаум, Х. Бос. . Современные операционные системы. СПб.: Питер, 2019, эл. рес.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

1. Естественные и технические науки;
2. Прикладная информатика.

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

1. <http://www.kremlin.ru/acts/bank/41460>;
2. <https://base.garant.ru/12148555/>;
3. <https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz>;
4. <http://www.kremlin.ru/acts/bank/42128>;
5. <https://docs.cntd.ru/document/1200181890>;
6. <https://docs.cntd.ru/document/1200179669>;
7. <https://docs.cntd.ru/document/1200194982>;
8. <https://digital-dpr.gosuslugi.ru/app/uploads/2025/03/metodika-oczenki-ubi-ot-5-fevralya-2021.pdf>;
9. <https://bdu.fstec.ru/threat>;
10. <https://e.lanbook.com/book/460715>;
11. <https://e.lanbook.com/book/217445>;
12. <https://www.piter.com/collection/razrabotka-i-realizatsiya-operatsiya-operatsionnyh-sistem-teoreticheskie-knigi-i-uchebniki/product/sovremennye-operatsionnye-sistemy-4-e-izd-2>;
13. <https://www.piter.com/collection/A28873/product/kompyuternye-seti-6-e-izd>;
14. <https://protect.gost.ru/gost/details/dc779444-7842-4f63-badd-db1a2ba90eb1>;
15. <https://protect.gost.ru/gost/details/89df2897-d0de-4015-a5b2-aee51b237a25>;
16. <https://protect.gost.ru/gost/details/0f42789b-012a-4795-9629-eef057adc0d0>;
17. https://nginx.org/en/docs/http/configuring_https_servers.html;
18. <https://www.postgresql.org/docs/current/user-manag.html>;
19. <https://nmap.org/docs.html>;
20. https://www.wireshark.org/docs/wsug_html_chunked/;
21. <https://docs.docker.com/>;
22. <https://portswigger.net/web-security>.

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;
2. Linux.

5.6. Информационные технологии:

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

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

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

6.2. Практические занятия:

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

6.3. Прочее:

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

Аннотация рабочей программы

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

Дисциплина нацелена на формирование *компетенций*:

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;

ПК-2.2 Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

Содержание дисциплины охватывает круг вопросов, связанных с нормативно-правовыми, организационными и техническими основами обеспечения информационной безопасности информационных систем. В рамках дисциплины рассматриваются основные понятия информационной безопасности, виды защищаемой информации, информационные активы, угрозы, уязвимости, риски и инциденты информационной безопасности.

Изучаются подходы к моделированию угроз и оценке рисков, основы криптографической защиты и защищённых сетевых соединений, принципы межсетевого экранирования, работа IDS/IPS, защита операционных систем и баз данных, основы безопасной разработки веб-приложений, мониторинг событий безопасности и реагирование на инциденты.

Практическая часть дисциплины выполняется на учебных изолированных стендах и направлена на закрепление навыков оценки рисков, настройки защищённого сетевого соединения, базового харденинга сервера, настройки правил межсетевого экранирования, регистрации сетевых событий, изучения признаков типовых уязвимостей веб-приложений и способов их предупреждения, а также рассмотрения признаков инцидента информационной безопасности по журналам событий и иным учебным материалам.

Итоговый практический кейс выполняется обучающимися в малых группах и является одним из контрольных мероприятий дисциплины. Промежуточная аттестация проводится в форме дифференцированного зачёта по сумме результатов контрольных мероприятий, выполненных в течение семестра. Оценка за итоговый практический кейс выставляется индивидуально каждому обучающемуся с учётом качества командного решения, личного вклада, содержания представленных материалов и ответов на вопросы при защите.

Программой дисциплины предусмотрены следующие **виды контроля**:

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

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к дифференцированному зачету.

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. Организационно-правовые основы и угрозы.		
Изучение нормативно-правовых основ информационной безопасности и требований к защите информации	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1,2)	6
Изучение подходов к идентификации информационных активов, моделированию угроз и оценке рисков		10
Итого по разделу 1		16
Раздел 2. Техническая защита информации.		
Изучение основ криптографической защиты информации и защищённых сетевых соединений	Э. Таненбаум, Х. Бос. . Современные операционные системы: СПб.: Питер, 2019 (2)	6
Изучение вопросов защиты операционных систем, баз данных и безопасного администрирования серверов		8
Итого по разделу 2		14
Раздел 3. Безопасность приложений и сетей.		
Изучение принципов сетевой безопасности, межсетевого экранирования, IDS/IPS и защиты периметра информационной системы	Е. В. Глинская, Н. В. Чичварин. . Информационная безопасность конструкций ЭВМ и систем: Москва: ИНФРА-М, 2021 (2)	6
Изучение методов сканирования сетей и проверки эффективности механизмов фильтрации в учебной среде		10
Изучение основ безопасной разработки веб-приложений, типовых уязвимостей и подходов DevSecOps		8
Обобщение результатов практических работ по сетевой безопасности и безопасности веб-приложений		4
Итого по разделу 3		28
Раздел 4. Реагирование на инциденты и итоговый практический кейс.		
Изучение основ мониторинга событий безопасности, киберустойчивости и реагирования на инциденты информационной безопасности	А. А. Бирюков. . Информационная безопасность: защита и нападение: М.: ДМК Пресс, 2017 (2) Е. В. Глинская, Н. В. Чичварин. . Информационная безопасность конструкций ЭВМ и систем: Москва: ИНФРА-М, 2021 (3)	8
Обобщение подходов к защите информационных систем и подготовка к итоговому практическому кейсу		4
Подготовка материалов для защиты		4

итогового практического кейса		
Итого по разделу 4		16

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- отчет по практическому заданию;
- вопросы к дифференцированному зачету;
- 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

По каждому практическому занятию 1–7 обучающийся представляет отчет в электронной форме. Отчет должен содержать цель работы, краткое описание выполненных действий, результаты выполнения задания, необходимые таблицы, скриншоты или фрагменты журналов, а также выводы по результатам работы.

Максимальное количество баллов за практические задания распределяется следующим образом:

- практическое занятие 1 – 10 баллов;
- практическое занятие 2 – 10 баллов;
- практическое занятие 3 – 8 баллов;
- практическое занятие 4 – 10 баллов;
- практическое занятие 5 – 14 баллов;
- практическое занятие 6 – 10 баллов;
- практическое занятие 7 – 10 баллов.

Итого за практические задания 1–7 – 72 балла.

Критерии оценивания отчета по практическому заданию:

- полнота выполнения задания;
- корректность выполненных действий и полученных результатов;
- обоснованность выводов и предложенных мер защиты;
- оформление отчета и соблюдение требований к представлению результатов;
- способность обучающегося пояснить выполненные действия и полученные результаты при защите отчета.

Распределение баллов по критериям осуществляется преподавателем с учетом максимального балла, установленного для соответствующего практического занятия, сложности задания и полноты представленных результатов.

Практическая работа считается сданной, если обучающийся набрал не менее минимального количества баллов, установленного для соответствующего практического занятия:

- практическое занятие 1 – не менее 6 баллов из 10;
- практическое занятие 2 – не менее 6 баллов из 10;
- практическое занятие 3 – не менее 5 баллов из 8;
- практическое занятие 4 – не менее 6 баллов из 10;
- практическое занятие 5 – не менее 9 баллов из 14;
- практическое занятие 6 – не менее 6 баллов из 10;
- практическое занятие 7 – не менее 6 баллов из 10.

В случае если практическая работа и отчет по ней выполнены своевременно, в полном объеме и в соответствии с установленными требованиями, а обучающийся при защите отчета даёт правильные ответы на вопросы преподавателя, выставляется максимальное количество баллов, установленное для соответствующего практического занятия.

Основаниями для снижения оценки являются:

- неполное выполнение задания;
- отсутствие обоснованных выводов;
- несоответствие отчета фактически выполненной работе;
- ошибки в применении терминов информационной безопасности;

- отсутствие подтверждающих материалов;
- невозможность пояснить выполненные действия и полученные результаты;
- нарушение требований к выполнению работы в учебной лабораторной среде.

Вопросы к дифференцированному зачету

Перечень теоретических вопросов к дифференцированному зачёту предоставляется преподавателем и размещается в учебно-методическом комплексе дисциплины.

При подготовке ответов на теоретические вопросы обучающимся рекомендуется использовать конспекты лекций, материалы практических занятий, учебно-методический комплекс дисциплины, а также источники основной и дополнительной литературы.

Дифференцированный зачет

Дифференцированный зачёт выставляется по сумме результатов контрольных мероприятий, проводимых в течение семестра. Максимальная сумма баллов за семестр составляет 100 баллов. Контрольные мероприятия включают выполнение практических заданий, представление отчётов по ним и защиту итогового практического кейса.

Набранная итоговая сумма баллов пересчитывается в оценку по следующей шкале:

- 86–100 баллов – «отлично»;
- 61–85 баллов – «хорошо»;
- 45–60 баллов – «удовлетворительно»;
- менее 45 баллов – «неудовлетворительно».

Итоговый практический кейс выполняется обучающимися в малых группах. Оценка за итоговый практический кейс выставляется индивидуально каждому обучающемуся с учётом качества командного решения, личного вклада, содержания представленных материалов и ответов на вопросы при защите. К защите итогового практического кейса допускается обучающийся, выполнивший обязательные практические работы 1–7 и представивший отчёты по ним.

В случае несогласия обучающегося с оценкой, выставленной по сумме набранных баллов, при условии выполнения практических работ 1–7 и участия в защите итогового практического кейса может быть проведено дополнительное устное собеседование по вопросам, размещённым в учебно-методическом комплексе дисциплины.

При невыполнении обязательных практических работ, отсутствии отчётов, невозможности подтвердить личный вклад в итоговый практический кейс или нарушении требований выполнения работ в учебной лабораторной среде обучающемуся выставляется оценка «неудовлетворительно».

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		ПК-2.1	ПК-2.2	
3	5	Раздел 1. Организационно-правовые основы и угрозы.	24	8	4	4	16	20	40	Отчет по практическому заданию
3	5	Раздел 2. Техническая защита информации.	21	7	4	3	14	25	20	Отчет по практическому заданию
3	5	Раздел 3. Безопасность приложений и сетей.	40	12	6	6	28	35	25	Отчет по практическому заданию
3	5	Раздел 4. Реагирование на инциденты и итоговый практический кейс.	23	7	3	4	16	20	15	Вопросы к дифференцированному зачету, Отчет по практическому заданию
Всего за 5 семестр			108	34	17	17	74	100	100	
Всего по дисциплине			108	34	17	17	74	100	100	

Оценочные материалы по дисциплине ОСНОВЫ 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

- № 1 Прочитайте текст и запишите развернутый обоснованный ответ
Объясните, зачем при оценке защищённости информационной системы необходимо учитывать требования стандартов и нормативных документов в области информационной безопасности. Приведите пример, как такие требования могут использоваться при проверке системы защиты.
- № 2 Прочитайте текст и запишите развернутый обоснованный ответ
Опишите порядок базового анализа защищённости информационной системы на учебном стенде. В ответе укажите, какие сведения необходимо собрать, какие защитные механизмы проверить и какие выводы должны быть отражены в отчёте.
- № 3 Прочитайте текст и установите соответствие
Установите соответствие между защитным механизмом и его назначением
- | | |
|---------------------------|--------------------------------------------------------------------|
| 1. Межсетевой экран | А. Защита сетевого соединения между клиентом и сервером |
| 2. IDS/IPS | Б. Фиксация значимых действий и событий в системе |
| 3. Журналирование событий | В. Фильтрация сетевого трафика по заданным правилам |
| 4. TLS | Г. Обнаружение или предотвращение нежелательной сетевой активности |
- № 4 Прочитайте текст и установите последовательность
Расположите этапы базовой проверки защищённости информационной системы в правильной последовательности.
1. Формирование выводов и рекомендаций
 2. Определение объекта проверки
 3. Проверка отдельных защитных механизмов
 4. Сбор сведений об активах, сервисах и настройках
 5. Фиксация результатов проверки
- № 5 Прочитайте текст и установите последовательность
Расположите действия при экспериментальной проверке работы межсетевого экрана и IDS/IPS на учебном стенде в правильной последовательности.
1. Сопоставить результаты проверки с журналами сетевых событий
 2. Настроить или проверить правила фильтрации
 3. Сформулировать вывод о достаточности настроенных механизмов защиты
 4. Выполнить проверку доступности разрешённых и запрещённых сервисов
 5. Зафиксировать срабатывания средств обнаружения
- № 6 Прочитайте текст и установите соответствие
Установите соответствие между элементом анализа защищённости и примером проверяемого результата
- | | |
|---------------------|------------------------------------------------------------------|
| Проверка правил МСЭ | А. Наличие записей о значимых действиях пользователей и сервисов |
| Проверка | Б. Наличие HTTPS-соединения и корректного использования |

защищённого соединения	сертификата
Проверка журналов событий	В. Доступны только разрешённые сетевые сервисы
Проверка прав доступа	Г. Пользователи не имеют избыточных полномочий

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

Какое средство используется для фильтрации сетевого трафика по заданным правилам?

Варианты ответа:

- А. Межсетевой экран
- Б. Текстовый редактор
- В. Архиватор
- Г. Графический редактор

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

Какую задачу выполняет журналирование событий безопасности?

Варианты ответа:

- А. Увеличивает скорость процессора
- Б. Фиксирует значимые действия и события в системе
- В. Удаляет все сетевые подключения
- Г. Заменяет резервное копирование

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

Какие действия относятся к проверке защищённости учебного стенда?

Варианты ответа:

- А. Проверка доступности сетевых сервисов
- Б. Рассмотрение журналов событий
- В. Проверка настроек доступа
- Г. Проведение действий в отношении внешних систем без разрешения
- Д. Оценка работы средств фильтрации

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

Для чего применяется TLS при работе веб-сервиса?

Варианты ответа:

- А. Для защиты сетевого соединения между клиентом и сервером
- Б. Для удаления журналов событий
- В. Для отключения базы данных
- Г. Для замены межсетевого экрана

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

Какие элементы могут проверяться при базовом анализе защищённости информационной системы?

Варианты ответа:

- А. Правила межсетевого экранирования
- Б. Журналы событий безопасности
- В. Права доступа пользователей
- Г. Цвет корпуса системного блока
- Д. Наличие защищённого сетевого соединения

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

Какие результаты должны быть отражены в отчёте по проверке защитных механизмов?

Варианты ответа:

- А. Описание выполненных действий
- Б. Полученные результаты проверки
- В. Обоснованные выводы
- Г. Предложения по снижению выявленных рисков
- Д. Случайные сведения, не относящиеся к заданию

ПК-2.2 - Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

№ 1 Прочитайте текст и запишите развернутый обоснованный ответ

Организация использует веб-сервис для приёма заявок от клиентов. В системе обрабатываются персональные данные клиентов, заявки, учётные записи сотрудников, журналы событий и резервные копии. Опишите, какие информационные ресурсы и компоненты объекта защиты подлежат защите, какие угрозы для них наиболее значимы и какие возможные пути реализации этих угроз следует учитывать при оценке объекта защиты.

№ 2 Прочитайте текст и запишите развернутый обоснованный ответ

Объясните, что понимается под информационным активом и почему определение информационных активов является первым этапом анализа объекта защиты.

№ 3 Прочитайте текст и установите соответствие

Установите соответствие между понятием и его содержанием.

- | | |
|-------------------------|-------------------------------------------------------------------------------------|
| 1. Информационный актив | А. Возможность причинения ущерба за счёт нарушения безопасности информации |
| 2. Угроза | Б. Слабое место, которое может быть использовано для реализации угрозы |
| 3. Уязвимость | В. Ресурс, имеющий ценность для организации и подлежащий защите |
| 4. Риск | Г. Возможность нарушения конфиденциальности, целостности или доступности информации |

№ 4 Прочитайте текст и установите соответствие

Установите соответствие между информационным активом и возможной угрозой.

- | | |
|----------------------------------|--------------------------------------------------------------------|
| 1. Учётная запись администратора | А. Несанкционированное изменение или раскрытие персональных данных |
| 2. База данных клиентов | Б. Недоступность сервиса для пользователей |
| 3. Журналы событий | В. Удаление сведений, необходимых для разбора инцидента |
| 4. Веб-сервис организации | Г. Получение расширенного доступа к системе |

№ 5 Прочитайте текст и установите последовательность

Расположите этапы определения угроз и рисков для объекта защиты в правильной последовательности.

Варианты:

- 1. Определение возможных угроз
- 2. Описание объекта защиты

3. Формирование перечня мер защиты
4. Определение информационных активов
5. Оценка рисков реализации угроз

№ 6 Прочитайте текст и установите последовательность

Расположите действия при подготовке аналитического заключения по учебному кейсу информационной безопасности в правильной последовательности.

Варианты:

1. Сформулировать выводы и рекомендации
2. Оценить риски и возможные последствия
3. Описать объект защиты и его назначение
4. Определить активы и значимые информационные ресурсы
5. Указать угрозы и возможные пути их реализации

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

Что означает доступность информации?

Варианты ответа:

- А. Информация доступна уполномоченным пользователям в нужное время
- Б. Информация скрыта от всех пользователей
- В. Информация всегда изменяется автоматически
- Г. Информация не подлежит защите

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

Какие элементы необходимо определить при анализе объекта защиты?

Варианты ответа:

- А. Информационные активы
- Б. Возможные угрозы
- В. Риски реализации угроз
- Г. Меры защиты
- Д. Случайные личные предпочтения пользователей, не влияющие на безопасность

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

Какие свойства относятся к базовым свойствам защищаемой информации?

Варианты ответа:

- А. Конфиденциальность
- Б. Целостность
- В. Доступность
- Г. Цветовое оформление интерфейса
- Д. Размер монитора

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

Какие меры могут снижать риски информационной безопасности?

Варианты ответа:

- А. Разграничение прав доступа
- Б. Журналирование событий
- В. Межсетевое экранирование
- Г. Использование защищённого сетевого соединения
- Д. Отключение всех средств защиты

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

Что относится к информационному активу организации?

Варианты ответа:

- А. База данных клиентов
- Б. Цвет стен в кабинете
- В. Личная кружка сотрудника
- Г. Номер аудитории

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

Какое свойство защищаемой информации нарушается при несанкционированном изменении данных?

Варианты ответа:

- А. Конфиденциальность
- Б. Целостность
- В. Доступность
- Г. Производительность