Приложение 2.27 к ОПОП по специальности
09.02.11 Разработка и управление программным обеспечением

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет
им. Г. И. Носова»
Многопрофильный колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 Основы информационной безопасности
«общепрофессионального цикла»
программы подготовки специалистов среднего звена
специальности 09.02.11 Разработка и управление программным обеспечением

Квалификация: Программист

Форма обучения
очная на базе основного общего образования

Рабочая программа учебной дисциплины «Основы информационной безопасности» разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Министерства просвещения Российской Федерации от «24» февраля 2025 г. № 138.

Организация-разработчик: Многопрофильный колледж ФГБОУ ВО «Магнитогорский государственный технический университет им. Г. И. Носова»

Разработчик:
преподаватель отделения №2 «Информационных технологий и транспорта»
Многопрофильного колледжа ФГБОУ ВО «МГТУ им. Г.И. Носова»
Кривонос Иван Алексеевич

ОДОБРЕНО

Предметно-цикловой комиссией «Информатики и вычислительной техники»
Председатель Ремез Т.Б.
Протокол № 5.1 от «11» февраля 2026г.

Методической комиссией МпК
Протокол № 4 от «18» февраля 2026г.

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель и место дисциплины в структуре образовательной программы

Рабочая программа учебной дисциплины «Основы информационной безопасности» является частью программы подготовки специалистов среднего звена по специальности 09.02.11 Разработка и управление программным обеспечением. Рабочая программа составлена для очной формы обучения.

Цель дисциплины: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «Основы информационной безопасности» включена в обязательную часть «общепрофессионального цикла» цикла образовательной программы по направленности «Веб-разработка».

1.2 Перечень планируемых результатов освоения дисциплины

Содержание дисциплины ориентировано на подготовку обучающихся к освоению видов деятельности программы подготовки специалистов среднего звена по специальности и овладению следующими профессиональными и общими компетенциями:

ПК 2.2. Разрабатывать модули программного обеспечения.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленной в разделе 4 ППССЗ.

Требования к результатам освоения дисциплины

Индекс и наименование ОК, ПК	**Результаты освоения**	
	Умеет	**Знает**
ПК 2.2. Разрабатывать модули программного обеспечения	Уд 3 ОП.05 Реализовывать защиту от распространенных уязвимостей (SQLi, XSS, CSRF); Уд 4_ОП.05 Применять безопасные практики аутентификации и управления сессиями; Уд5_ОП.05 Использовать средства статического и динамического анализа кода	Зд 4 ОП.05. Классификация уязвимостей (CVE, CWE) и стандарты их оценки (CVSS); Зд 5_ОП.05. Механизмы защиты веб-приложений и API; Зд 6_ОП0.05 Принципы безопасного кодирования и работы с конфиденциальными данными
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	Уо 02.02 использовать современное программное обеспечение, различные цифровые средства для решения профессиональных задач; проявлять культуру информационной безопасности при использовании информационно-коммуникационных технологий;	Зо 02.02 современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;

1.3 Обоснование часов учебной дисциплины в рамках вариативной части

Дополнительные профессиональные компетенции	Дополнительные знания, умения, навыки	Номер и наименование темы	Объем часов	Обоснование включения в рабочую программу
-	Зд 6_ОП.05	Тема 1 Введение в	2	Тема расширяет и

		информационную безопасность		углубляет базовые знания в области информационной безопасности, формируя фундаментальные компетенции, необходимые для защиты программного обеспечения на всех этапах жизненного цикла.
-	Зд 4_ОП.05	Тема 2 Управление безопасностью информации	2	Тема обеспечивает практическую подготовку по классификации и оценке уязвимостей ПО в соответствии с международными стандартами, а также знакомит с лучшими практиками безопасной разработки для интеграции процессов защиты в жизненный цикл ПО
-	Уд 4_ОП.05 Зд 6_ОП.05	Тема 3 Криптография	2	Тема формирует практические навыки применения симметричного и асимметричного шифрования, хеширования и управления ключами для обеспечения конфиденциальности и целостности данных в разрабатываемом ПО.
-	Уд 3_ОП.05 Зд 5_ОП.05	Тема 4 Защита сетевой инфраструктуры	2	Тема развивает практические навыки реализации защитных механизмов и тестирования безопасности для обеспечения устойчивости программного обеспечения к кибератакам.
-	Уд 3_ОП.05 Уд 4_ОП.05	Тема 5 Безопасность приложений	2	Тема формирует компетенции по

	Уд 5_ОП.05 Зд 4_ОП.05 Зд 6_ОП.05			безопасному кодированию и анализу защищенности прикладного ПО, что критически важно для предотвращения распространенных классов уязвимостей (OWASP Top 10).
-	Уд 4_ОП.05 Зд 6_ОП.05	Тема 6 Защита данных	2	Тема формирует компетенции по автоматизированному анализу безопасности кода для своевременного выявления и устранения уязвимостей на различных этапах разработки.
-	Уд 5_ОП.05 Зд 5_ОП.05	Тема 7 Безопасность облачных технологий	2	Тема обеспечивает формирование умений безопасного программирования и управления конфигурациями для минимизации рисков компрометации программного обеспечения.
-	Уд 5_ОП.05 Зд 4_ОП.05	Тема 8 Инциденты безопасности	2	Тема расширяет компетенции в области защиты современных распределенных систем и API для обеспечения безопасности облачных и микросервисных архитектур.
	Зо 02.02	Тема 9 Социальная инженерия и человеческий фактор	1	Тема дополняет технические аспекты безопасности знаниями о психологических методах атак, формируя навыки защиты от социальной инженерии как одного из самых актуальных векторов

				взлома ПО.
	Зо 02.02	Тема 10 Будущее информационной безопасности	1	Тема обеспечивает понимание актуальных трендов (ИИ, квантовые вычисления, Zero Trust) и перспективных угроз, что необходимо для формирования долгосрочных профессиональных компетенций выпускника.
Всего академических часов учебной дисциплины в рамках вариативной части			18	

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	**Объем в часах**	**в т.ч. в форме практической подготовки**
теоретические занятия (лекции, уроки)	18	не предусмотрено
практические занятия	не предусмотрено	не предусмотрено
лабораторные занятия	36	36
самостоятельная работа	не предусмотрено	не предусмотрено
промежуточная аттестация	не предусмотрено	не предусмотрено
Форма промежуточной аттестации – зачет с оценкой		

2.2 Тематический план и содержание учебной дисциплины

Наименование разделов и тем учебной дисциплины	Содержание учебного материала, практические и лабораторные занятия, самостоятельная работа обучающихся	Объем, акад. ч / в том числе в форме практической подготовки, акад.ч.	Код ПК, ОК	Коды осваиваемых элементов компетенций
1	2	3	4	5
Тема 1 Введение в информационную безопасность	**Содержание**	2/0		
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	2/0	ОК 02	Уо 02.02 Зо 02.02
Тема 2 Управление безопасностью информации	**Содержание**	2/0		
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2/0	ОК 02	Уо 02.02 Зо 02.02
Тема 3 Криптография	**Содержание**	2/0		
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2/0	ПК 2.2 ОК 02	Зд 6_ОП.05 Уо 02.02
Тема 4 Защита сетевой инфраструктуры	**Содержание**	14/12		
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2/0	ПК 2.2 ОК 02	Зд 5_ОП.05 Уд 3_ОП.05
	В том числе лабораторных занятий	**12/12**		
	Лабораторная работа №1. Организация защиты от атак	6/6	ПК 2.2 ОК 02	Зд 5_ОП.05 Уд 3_ОП.05
	Лабораторная работа №2. Организация работы VPN и межсетевого экрана	6/6	ПК 2.2 ОК 02	Зд 5_ОП.05 Уд 3_ОП.05
Тема 5 Безопасность приложений	**Содержание**	8/6		
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2/0	ПК 2.2 ОК 02	Уд 3_ОП.05 Уд 4_ОП.05 Уд 5_ОП.05 Зд 4_ОП.05 Зд 6_ОП.05
	В том числе лабораторных занятий	**6/6**		

	Лабораторная работа №3. Тестирование на проникновение и анализ уязвимостей.	6/6	ПК 2.2 ОК 02	Уд 5_ОП.05 Зд 4_ОП.05
Тема 6 Защита данных	**Содержание**	10/8		
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2/0	ПК 2.2 ОК 02	Уд 4_ОП.05 Зд 6_ОП.05
	В том числе лабораторных занятий	**8/8**		
	Лабораторная работа №4. Выполнение резервного копирования и восстановления данных. Управление доступом к данным	8/8	ПК 2.2 ОК 02	Уд 4_ОП.05 Зд 6_ОП.05
Тема 7 Безопасность облачных технологий	**Содержание**	4/2		
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2/0	ПК 2.2 ОК 02	Зд 5_ОП.05 Уо 02.02
	В том числе лабораторных занятий	**2/2**		
	Лабораторная работа №5 Изучение модели облачных услуг и их безопасности	2/2	ПК 2.2 ОК 02	Зд 5_ОП.05 Уо 02.02
Тема 8 Инциденты безопасности	**Содержание**	8/6		
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2/0	ПК 2.2 ОК 02	Уд 5_ОП.05 Зд 4_ОП.05
	В том числе лабораторных занятий	**6/6**		
	Лабораторная работа №6 Работа с инцидентами.	6/6	ПК 2.2 ОК 02	Уд 5_ОП.05 Зд 4_ОП.05
Тема 9 Социальная инженерия и человеческий фактор	**Содержание**	3/2		
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	1/0	ОК 02	Уо 02.02 Зо 02.02
	В том числе лабораторных занятий	**2/2**		
	Лабораторная работа №7 Разработка политики информационной безопасности	2/2	ОК 02	Уо 02.02 Зо 02.02
Тема 10 Будущее информационной безопасности	**Содержание**	1/0		
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	1/0	ОК 02	Зо 02.02
Всего		**54/36**		

2.3 Перечень практических и лабораторных занятий

Номенклатура практических и лабораторных занятий должна обеспечивать освоение названных в разделе 1.2 рабочей программы умений.

Темы лабораторных и практических занятий	Содержание (краткое описание)	Специализированное оборудование, технические средства, программное обеспечение
Лабораторные занятия		
Лабораторная работа №1. Организация защиты от атак	Формирование умений выявлять актуальные киберугрозы (фишинг, вредоносное ПО, сетевые атаки) и подбирать организационно-технические меры защиты	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V) OWASP Threat Dragon (моделирование угроз), Draw.io, матрица угроз MITRE ATT&CK
Лабораторная работа №2. Организация работы VPN и межсетевого экрана	Формирование умений настройки VPN-туннелей, правил межсетевого экрана (iptables, фаерволлы) и оценки эффективности фильтрации трафика	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V) Виртуальные машины (VMware/VirtualBox), OpenVPN, WireGuard, iptables/nftables, pfSense, Wireshark
Лабораторная работа №3. Тестирование на проникновение и анализ уязвимостей.	Формирование умений проводить тестирование на проникновение (pentest), сканирование уязвимостей и оценку их критичности с использованием CVSS	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V) CVSS Calculator (NVD), OWASP ZAP, Burp Suite Community, Nmap, Metasploit (опционально), Kali Linux
Лабораторная работа №4. Выполнение резервного копирования и восстановления данных. Управление доступом к данным	Формирование умений настройки резервного копирования (полное, инкрементное, дифференциальное), восстановления данных и управления	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V)

	правами доступа (RBAC, ACL)	Системы резервного копирования (Bacula, Duplicati, rsync), ОС Windows/Linux (NTFS permissions, chmod, setfacl), облачные хранилища (S3, Nextcloud)
Лабораторная работа №5 Изучение модели облачных услуг и их безопасности	Формирование умений анализа моделей облачного обслуживания (IaaS, PaaS, SaaS), оценки угроз для облачных сред и настройки базовых средств защиты	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V) Интернет-браузер, консоли облачных провайдеров (Yandex Cloud, AWS Free Tier, Microsoft Azure), документация CSA, OWASP Cloud Security
Лабораторная работа №6 Работа с инцидентами.	Формирование умений обнаружения, классификации, расследования и реагирования на инциденты ИБ с использованием SIEM-систем	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V) TheHive, MISP (платформа обмена угрозами), ELK Stack (Elasticsearch, Logstash, Kibana), Syslog-ng, демонстрационные стенды с логами
Лабораторная работа №7 Разработка политики информационной безопасности	Формирование умений разработки и документирования корпоративной политики ИБ, парольной политики, правил доступа и планов реагирования на инциденты	ПК (Процессор: Intel(R) Core(TM) i5-9400 CPU @2.90GHz 2.90 GHz/RAM 8,00 Gb /HDD. Монитор IIYAMA 24 дюйма Монитор: PHILIPS 243V) Текстовые процессоры (MS Word, LibreOffice Writer), шаблоны политик (ISO 27001, NIST, ФСТЭК), конструкторы документов, системы контроля версий (Git)

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Материально-техническое обеспечение

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория «Программного обеспечения и сопровождения компьютерных и информационных систем», оснащенная в соответствии с приложением 3 образовательной программы.

Помещение для воспитательной работы, оснащенное в соответствии с приложением 3 образовательной программы.

Компьютерный класс, оснащенный в соответствии с приложением 3 образовательной программы.

3.2 Учебно-методическое и информационное обеспечение реализации программы

Основные источники:

1. Зегжда, Д. П. Безопасность информационных систем : учебник / Д. П. Зегжда, Н. А. Ивашко. — Москва : КноРус, 2025. — 310 с. — ISBN 978-5-406-14855-6. — URL: https://book.ru/book/957955. — Текст : электронный (посещался 17 марта 2026 года).

2. Смирнов, С. Н. Защита информационных систем : учебное пособие / С. Н. Смирнов. — Москва : КноРус, 2024. — 275 с. — ISBN 978-5-406-13412-2. — URL: https://book.ru/book/955650. — Текст : электронный (посещался 17 марта 2026 года).

3. Чернов, А. В. Информационная безопасность систем и сетей : учебник / А. В. Чернов. — Москва : КноРус, 2026. — 330 с. — ISBN 978-5-406-16245-3. — URL: https://book.ru/book/962210. — Текст : электронный (посещался 17 марта 2026 года).

Дополнительные источники:

1. Костин, В. Н. Безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : КноРус, 2025. — 260 с. — ISBN 978-5-406-14675-0. — URL: https://book.ru/book/957610. — Текст : электронный (посещался 17 марта 2026 года).

2. Федоров, А. Л. Методы и средства защиты информации в информационных системах : учебное пособие / А. Л. Федоров. — Москва : КноРус, 2024. — 290 с. — ISBN 978-5-406-13388-0. — URL: https://book.ru/book/955405. — Текст : электронный (посещался 17 марта 2026 года).

Периодические издания:

1. Журнал «Информационная безопасность» (посещался 17 марта 2026 года)
2. Журнал «Защита информации. Инсайд» (посещался 17 марта 2026 года)

Интернет-ресурсы:

1. POWASP Open Web Application Security Project [Электронный ресурс] – Режим доступа: https://owasp.org, свободный. – Загл. с экрана. – Яз. англ (посещался 17 марта 2026 года)
2. CVE Common Vulnerabilities and Exposures [Электронный ресурс] – Режим доступа: https://cve.mitre.org, свободный. – Загл. с экрана. – Яз.англ (посещался 17 марта 2026 года).
3. NVD National Vulnerability Database [Электронный ресурс] – Режим доступа: https://nvd.nist.gov, свободный. – Загл. с экрана. – Яз. англ (посещался 17 марта 2026 года)
4. ФСТЭК России: Федеральная служба по техническому и экспортному контролю [Электронный ресурс] – Режим доступа: https://fstec.ru, свободный. – Загл. с экрана. – Яз. рус. (посещался 17 марта 2026 года)
5. Хабр: Публикации о информационных технологиях и информационной безопасности [Электронный ресурс] – Режим доступа: https://habr.com, свободный. – Загл. с экрана. – Яз. Рус (посещался 17 марта 2026 года)

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе текущего контроля и промежуточной аттестации.

4.1 Текущий контроль

№	Контролируемые разделы (темы) учебной дисциплины	Контролируемые результаты	Наименование оценочного средства	Критерии оценки
1	Раздел 1 Введение в безопасность программного обеспечения	ПК 2.2, ОК02	Тестирование	См. ниже
2	Раздел 2 Модели угроз и анализ рисков	ПК 2.2, ОК02	Лабораторная работа	См.ниже
3	Раздел 3 Безопасная разработка программного обеспечения	ПК 2.2, ОК03	Лабораторное задание	См.ниже
4	Раздел 4 Анализ безопасности программного обеспечения	ПК 2.2, ОК02	Лабораторная работа	См.ниже
5	Раздел 5 Защита программного обеспечения	ПК 2.2, ОК02	Лабораторная работа	См.ниже

Критерии оценки лабораторного задания:

«5» (отлично): выставляется студенту, если практическая работа в полном объеме, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач.

«4» (хорошо): выставляется студенту, если при выполнении задания допущены незначительные ошибки, решение оформлено с соблюдением установленных правил; студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач;

«3» (удовлетворительно): выставляется студенту, если задание выполнено с «грубыми» ошибками, решение оформлено без соблюдения установленных правил;

«2» (неудовлетворительно): выставляется студенту, если работа не выполнена.

Критерии оценки тестирования:

За правильно выполненное действие, задание выставляется положительная оценка – 1 балл.

За неправильно выполненное действие, задание выставляется отрицательная оценка – 0 баллов.

Для оценки образовательных достижений обучающихся применяется универсальная шкала.

Процент результативности (правильных ответов)	Качественная оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

4.2 Промежуточная аттестация

Промежуточная аттестация обучающихся осуществляется по завершении изучения дисциплины и позволяет определить качество и уровень ее освоения.

Форма промежуточной аттестации по дисциплине «Основы информационной безопасности» - зачет с оценкой.

Результаты обучения	Оценочные средства для промежуточной аттестации
ПК 2.2 ОК 02	Устный опрос по билетам 1. Основные понятия информационной безопасности. Цели и задачи защиты информации.

	2. Виды угроз информационной безопасности и их классификация. 3. Нормативно-правовое обеспечение информационной безопасности. 4. Модели угроз и методы анализа рисков. 5. Основы криптографии: симметричное и асимметричное шифрование. 6. Хэширование и цифровая подпись. 7. Основные уязвимости веб-приложений (OWASP Top 10). 8. SQL-инъекции, XSS, CSRF: принципы атак и методы защиты. 9. Принципы безопасного программирования. 10. Методы тестирования безопасности (статический и динамический анализ). 11. Защита сетевой инфраструктуры (VPN, firewall). 12. DDoS и MITM-атаки: принципы и защита. 13. Защита данных: шифрование, резервное копирование. 14. Управление доступом (RBAC, ACL). 15. Безопасность облачных технологий (IaaS, PaaS, SaaS). 16. Реагирование на инциденты информационной безопасности. 17. Основы цифровой криминалистики (форензика). 18. Социальная инженерия и методы защиты от нее. 19. Политика информационной безопасности организации. 20. Современные тенденции ИБ (AI, Zero Trust). 21. Классификация уязвимостей (CVE, CWE) и их назначение. 22. Метрика CVSS и оценка критичности уязвимостей. 23. Принципы работы аутентификации и авторизации. 24. Управление сессиями в веб-приложениях. 25. Многофакторная аутентификация и ее преимущества. 26. Основные инструменты статического анализа кода. 27. Основные инструменты динамического анализа безопасности. 28. Понятие DevSecOps и его роль в разработке ПО. 29. Жизненный цикл безопасной разработки (SDL). 30. Контроль целостности данных и методы его обеспечения. 31. Протоколы защищенной передачи данных (HTTPS, TLS). 32. Работа межсетевых экранов и их виды. 33. Системы обнаружения и предотвращения атак (IDS/IPS). 34. Логирование и мониторинг событий безопасности. 35. SIEM-системы и их назначение. 36. Основные этапы реагирования на инциденты. 37. Резервное копирование: виды и стратегии. 38. Управление ключами в криптографии. 39. Безопасность API и методы ее обеспечения. 40. Основные принципы модели Zero Trust.

Критерии оценки зачёта с оценкой

«Отлично» – студент полно и грамотно раскрывает вопрос, демонстрирует системные знания, приводит примеры практического применения, уверенно отвечает на дополнительные вопросы.

«Хорошо» – студент раскрывает вопрос в полном объеме, допускает незначительные неточности, в целом владеет материалом.

«Удовлетворительно» – студент раскрывает вопрос частично, допускает ошибки, испытывает затруднения при ответах на дополнительные вопросы.

«Неудовлетворительно» – студент не раскрывает содержание вопроса, демонстрирует фрагментарные знания или их отсутствие.

Приложение 1

ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При проведении теоретических и практических/лабораторных занятий используются следующие педагогические технологии:

№ п/п	Название образовательной технологии (с указанием автора)	Цель использования образовательной технологии	Планируемый результат использования образовательной технологии	Описание порядка использования (алгоритм применения) технологии в практической профессиональной деятельности
1	Информационно коммуникационные технологии (Гарольд Дж. Ливитт и Томас Л. Уислер)	Повышение качества обучения за счет внедрения современных технологий	Повышение эффективности процесса обучени	В ходе лабораторных занятий применяются современное программное обеспечение и прикладные программы для анализа защищенности (SonarQube, OWASP ZAP, Dependency-Check)
2	Проектное обучение	Формирование компетенций по комплексной защите информационных систем	Развитие умений применять методы защиты информации на практик	Выполнение сквозного проекта по анализу угроз и реализации защиты типового веб-приложения с полным циклом от моделирования угроз до тестирования на проникновение