

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тамбовский государственный университет имени Г.Р. Державина»
Институт экономики, информационных технологий и креативных индустрий
Факультет информационных технологий и экономики
Кафедра математического моделирования и информационных технологий



УТВЕРЖДАЮ:
Директор института
Кожевникова Т.М.
«03» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОП.5 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы среднего профессионального образования – программа подготовки специалистов среднего звена по специальности

09.02.11 «Разработка и управление программным обеспечением»

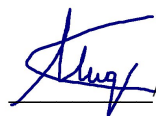
Направленность: Веб-разработка

Квалификация
Программист

Год набора 2026

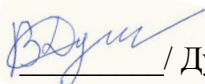
Тамбов –2026

Разработчик(и) программы:



/ Сидляр М.Ю., старший преподаватель кафедры математического моделирования и информационных технологий

Эксперт:



/ Дудаков В.П., системный администратор ООО «Европа-Европа 33», к.т.н., доцент

Рабочая программа разработана на основе ФГОС СПО и утверждена на заседании кафедры математического моделирования и информационных технологий «02» февраля 2026 года протокол № 6

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	9
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	10

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением.

Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1.	Проектировать базы данных.
ПК 1.4.	Администрировать базы данных.
ПК 1.5.	Защищать информацию в базе данных с использованием технологии защиты информации.
ПК 3.1.	Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика.
ПК 3.2.	Разрабатывать веб-приложения в соответствии с техническим заданием.
ПК 3.3.	Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием.
ПК 3.5.	Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности.
ПК 3.7.	Реализовывать мероприятия по продвижению приложения.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 01 ОК 02 ОК 09 ПК 1.1. ПК 1.4. ПК 1.5. ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.5. ПК 3.7.	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составлять план действия; определять необходимые ресурсы;	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности номенклатура информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства

- владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) определять задачи для поиска информации; определять необходимые источники информации; - планировать процесс поиска; - структурировать получаемую информацию; - выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; - оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач понимать тексты на базовые профессиональные темы - шифровать данные и обеспечивать их конфиденциальность - анализ требований безопасности информационных систем - разрабатывать и реализовывать меры безопасности - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	- информатизации; - порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств. - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности - принципы безопасности хранения данных - методы защиты баз данных от внешних угроз - принципы криптографии и методов шифрования данных - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных - законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др. - отраслевая нормативная техническая документация - источники информации, необходимой для профессиональной деятельности - современный отечественный и зарубежный опыт в профессиональной деятельности - принципы и методы обеспечения безопасности информационных систем - принципов безопасности информационных систем - современных методов и технологий в области безопасности информационных систем - законодательных и нормативных актов в области безопасности информационных систем - источники угроз информационной безопасности и меры по их предотвращению - основные угрозы безопасности мобильных приложений - принципы криптографии и шифрования данных. - стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenIDConnect - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA - основные принципы безопасности информации и методов ее защиты. - стандартные криптографические алгоритмы для шифрования данных принципы обеспечения безопасности передачи данных по сети - основы безопасности приложений и инфраструктуры методы анализа на уязвимости и мониторинга безопасности знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения - знание инструментов и технологий для
--	--

		обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы
--	--	--

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	106
в т.ч. в форме практической подготовки	-
в т. ч.:	
теоретическое обучение	44
практические занятия	44
<i>Самостоятельная работа</i>	-
Промежуточная аттестация в форме экзамена	18

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Коды компетенций, формированию которых способствует элемент программы
Тема 1.1. Введение в информационную безопасность	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности		
Тема 1.2. Управление безопасностью информации	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)		
Тема 1.3. Криптография	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		
	Практические и лабораторные занятия Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	6	
Тема 1.4. Защита сетевой инфраструктуры	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов		
	Практические и лабораторные занятия Организация защиты от атак Организация работы VPN и межсетевого экрана	6	
Тема 1.5. Безопасность приложений	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Уязвимости веб-приложений (OWASP TopTen). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		
	Практические и лабораторные занятия Тестирование на проникновение и анализ уязвимостей.	6	
Тема 1.6. Защита данных	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		
	Практические и лабораторные занятия Выполнение резервного копирования и восстановления данных. Управление доступом к данным	6	
Тема 1.7. Безопасность	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1.,
	Особенности безопасности в облачных средах.		

облачных технологий	Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	6	ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Практические и лабораторные занятия		
	Изучение модели облачных услуг и их безопасности		
Тема 1.8. Инциденты безопасности	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		
	Практические и лабораторные занятия		
	Работа с инцидентами.	6	
Тема 1.9. Социальная инженерия и человеческий фактор	Содержание	4	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности		
	Практические и лабораторные занятия	8	
	Разработка политики информационной безопасности		
Тема 1.10. Будущее информационной безопасности	Содержание	8	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.4., ПК 1.5., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.5., ПК 3.7.
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		
Промежуточная аттестация - экзамен		18	
Всего		106	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная необходимым для реализации программы учебной дисциплины оборудованием:

- Посадочные места по количеству обучающихся (столы, стулья)
- Рабочее место преподавателя
- Шкаф или полки для хранения учебной и методической литературы
- Доска маркерная
- ПК преподавателя (системный блок, монитор, клавиатура, мышь)
- ПК (системный блок, монитор, клавиатура, мышь) по количеству обучающихся
- Мультимедийный проектор
- Аудио- и видеооборудование
- Комплект учебно-методических материалов

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные и/или электронные издания

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/394547> (дата обращения: 16.11.2024).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/414950> (дата обращения: 16.11.2024).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/195510> (дата обращения: 16.11.2024)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/385082> (дата обращения: 16.11.2024)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Критерии и методы оценивания

Результаты обучения	Показатели освоённости компетенций	Методы оценки
Знает: - актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств	Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить; Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; Знает алгоритмы выполнения работ в профессиональной и смежных областях; Знает методы работы в профессиональной и смежных сферах; Знает структуру плана для решения задач; Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; Знает приемы структурирования информации; Знает формат оформления результатов поиска информации, современные средства и устройства информатизации; Может применять современные средства и	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - принципы безопасности хранения данных; - методы защиты баз данных от внешних угроз - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных - законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в	устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; Знает принципы безопасности хранения данных; Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный	
---	---	--

профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем; - законодательные и нормативные акты в области безопасности информационных систем; - источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных; - стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenIDConnect; - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи	отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в области безопасности информационных систем; Знает законодательные и нормативные акты в области безопасности информационных систем; Знает источники угроз информационной безопасности и меры по их предотвращению; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenIDConnect; Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; Владеет основными принципами безопасности информации и методов ее защиты; Знает стандартные криптографические алгоритмы для шифрования	
---	---	--

данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. Умеет: -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; -составлять план	данных; Имеет представление о принципах обеспечения безопасности передачи данных по сети; Знает основы безопасности приложений и инфраструктуры; Знает методы анализа на уязвимости и мониторинга безопасности; Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализирует задачу и/или проблему и может выделить её составные части; Умеет определять этапы решения задачи; Может выявлять и эффективно искать	
--	--	--

действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи для поиска информации; - определять необходимые источники информации; - планировать процесс поиска; - структурировать получаемую информацию; - выделять наиболее значимое в перечне информации; - оценивать практическую значимость результатов поиска; - оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы;	информацию, необходимую для решения задачи и/или проблемы; Составляет план действия; Может определять необходимые ресурсы; Владеет актуальными методами работы в профессиональной и смежных сферах; Может реализовывать составленный план; Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); Умеет определять задачи для поиска информации; Умеет определять необходимые источники информации; Планирует процесс поиска; Умеет структурировать получаемую информацию; Может выделить наиболее значимое в перечне информации; Умеет оценивать практическую значимость результатов поиска; Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач; Может использовать современное программное обеспечение; Может использовать различные цифровые средства для решения	
--	---	--

- шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	профессиональных задач; Понимает тексты на базовые профессиональные темы; Умеет шифровать данные и обеспечивать их конфиденциальность; Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	
---	--	--

4.2 Типовые оценочные средства текущего контроля Тестирование

ТЕСТ (Вариант №1)

1. Каким Указом Президента утверждена Стратегия национальной безопасности РФ?
 - A. №693 от 26 декабря 2015 года
 - B. №613 от 26 февраля 2000 года
 - C. №683 от 31 декабря 2015 года
 - D. №623 от 31 декабря 2015 года
2. Какая страна мира является самой крупной по площади территории?
 - A. Россия
 - B. Канада
 - C. Китай
 - D. США
3. Какая страна мира является самой крупной по населению?
 - A. Индия
 - B. США
 - C. КНР
 - D. Индонезия
4. Первая концепция сетецентрической войны носит название?
 - A. Три квадрата генерала Шеридана
 - B. Пять колец полковника Уордена
 - C. Четыре зоны майора Панкрафта
 - D. Шесть измерений концепции Уоррена
5. Какая страна не входит в БРИКС?
 - A. ЮАР
 - B. Бразилия
 - C. Индия
 - D. Казахстан
6. С каким союзом не партнерствует ШОС?
 - A. ООН
 - B. НАТО

- C. ОДКБ
- D. АСЕАН

7. Что является разновидностью боевых действий, в которых ключевым объектом воздействия является информация, хранящаяся или циркулирующая в управляющих, разведывательных, боевых и прочих системах противника?

- A. Информационная война
- B. Кибернетическая революция
- C. Психологическая операция
- D. Дезинформация

8. Какие виды информационных атак существуют?

- A. Логические и бинарные
- B. Прямые и обратные
- C. Обратимые и необратимые
- D. Прямые и косвенные

9. Психологическое воздействие на гражданское население и (или) военнослужащих другого государства с целью достижения политических или чисто военных целей это?

- A. Патогенная война
- B. Физиологическая война
- C. Психологическая война
- D. "Горячая" война

10. Информационное воздействие направлено на?

- A. Создание "информационного шума"
- B. Модификацию ментальных моделей (моделей мира) людей
- C. Пропаганду здорового образа жизни
- D. Выявление уязвимостей и угроз, являющихся причиной риска

11. В каком году была принята Будапештская конвенция о компьютерных преступлениях ?

- A. 1985
- B. 2006
- C. 2017
- D. 2001

12. Действующая Доктрина информационной безопасности РФ утверждена Указом Президента

- A. №646 от 5 декабря 2016 г.
- B. N ПР1895 от 9 сентября 2000 г.
- C. №683 от 31 декабря 2015 года
- D. №646 от 31 января 2016 года

Тест (Вариант №2)

1. Основным международным стандартом регламентирующим ВСМ является

- A. ISO/IEC 18044
- B. ISO/IEC 15408
- C. PAS56
- D. BS25999

2. Какая стратегия защиты используется если возможные потери велики и риск высокий

- A. Разработка планов ВСМ
- B. Отказ от ответственности
- C. Мониторинг и реагирование
- D. Принять риски и возможные потери

3. Что такое RTO?

- A. Время за которое можно позволить потери информации
- B. Время которое можно потратить на восстановление деятельности

- C. Уровень доверия, обеспечиваемый механизмом безопасности
D. Соотношение затрат / выгод
4. К детерминированным качественным методам анализа риска относится
A. Анализ вида, последствий и критичности отказа
B. Методика анализа эффекта домино
C. Анализ ошибочных действий
D. Методика определения и оценки потенциального риска
5. Как рассчитать остаточный риск?
A. Угрозы x Риски x Ценность актива
B. (Угрозы x Ценность актива x Уязвимости) x Риски
C. $SLE \times Частоту = ALE$
D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля
6. Что не относится к ТСБ?
A. СКУД
B. СОС
C. СВК
D. САЗ
7. Конфиденциальная информация это?
A. документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
B. обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя
C. обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания
D. Информация о государственных заказах и оборонной деятельности
8. Какой класс защиты имеют ОС Windows согласно "Оранжевой книге"
A. B1
B. D2
C. C2
D. B3
9. Какие отечественные суперкомпьютеры производит предприятие "ТПлатформы"?
A. ЕС1870
B. СКИФ
C. Эльбрус401
D. ЕС1703
10. Какое российское предприятие производит нейроускорители на базе нейрочипов?
A. НИИЦЭВТ
B. ВНИИНС им. Соломатина
C. ФакторТС
D. НТЦ "Модуль"
11. Какой элемент не используется для создания квантовых компьютеров?
A. Адамара
B. Тоффли
C. Экерта
D. Паули
12. Что не включает в себя формальная модель информационного потока?
A. множество предикатов
B. множество объектов
C. множество субъектов
D. отношение потоков

Тест (Вариант №3)

1. Под политикой безопасности понимается?

- A. Список стандартов, процедур и политик для разработки программы безопасности
- B. Информация, технические и программные средства, обслуживающий персонал и пользователи
- C. Структура, разработанная для снижения воздействия угроз в компаниях
- D. Совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы

2. К моделям политик безопасности относятся

- A. Дискреционные (произвольные), мандатные (нормативные)
- B. Модели на основе методов морфологического ящика
- C. Модели на основе теории статистических решающих функций
- D. Модели на основе математической теории систем М. Месаровича

3. К угрозам целостности информации относятся:

- A. Физическое повреждение или разрушение оборудования и носителей данных
- B. Кражи и подлоги в информационной сфере
- C. Протечки водопровода или отопительных систем, выход кондиционеров из строя и т. п.
- D. Искажения и модификации данных

4. Что не является источником угроз НСД?

- A. Аппаратная закладка
- B. Владелец информации
- C. Нарушитель
- D. Носитель вредоносной программы

5. Кто не является внешним нарушителем?

- A. Криминальные структуры
- B. Разведывательные службы
- C. Недобросовестные партнеры
- D. Системный администратор сегмента сети

6. Что не является основным признаком классификации уязвимостей ПО?

- A. Тип программного обеспечения
- B. Причина возникновения
- C. Последствия использования уязвимостей
- D. По характеру последствий от реализации угроз

7. Что относится к достоинствам мандатного разграничения доступа?

- A. Простота и ясность определения правил разграничения доступа для разработчиков и пользователей компьютерной системы
- B. Снижение эффективности компьютерной системы
- C. Проверка прав доступа субъекта к объекту производится в момент открытия этого объекта
- D. Статичность разграничения доступа

8. Согласно руководящему документу ФСТЭК, для каких классов АС должен осуществляться контроль доступа к защищаемым ресурсам только с помощью дискреционного разграничения доступа?

- A. 1А
- B. 1В, 1Б, 1А
- C. 1Г
- D. 1В

9. Какое средство аутентификации требует ввода биометрических данных?

- A. ruToken
- B. Мышь "Magicsecure 3100"
- C. Электронный замок "Соболь"

D. eToken

10. В основу проекта ADEPT50 положена формальная модель управления защитой, обеспечивающая управление четырьмя видами объектов защиты. Что не является объектом?

A. терминал (t)

B. задание (j)

C. папка (p)

D. файл (f)

11. Нарушения каких типов можно обнаружить с помощью NIDX?

A. Попытки внешнего и внутреннего взлома

B. Несанкционированная модификация

C. Несанкционированное чтение и копирование

D. Все вышеперечисленное верно

12. У 1й категории внутренних нарушителей отсутствует следующая возможность.

A. Изменение конфигурации технических средств

B. Обладает возможностями внесения закладок в технические средства на всех стадиях жизненного цикла

C. Имеет доступ к фрагментам информации

D. Располагает фрагментами информации о топологии ИС

4.3 Промежуточная аттестация по дисциплине

Вопросы для экзамена

1. Современное понимание и структура ИБ, динамика развития, источники проблем, противоречия. Положение России в современном мире.

2 Технические, социальные и социотехнические аспекты ИБ, их взаимосвязь

3 Понятия информационной войны, информационного террора, информационной преступности – технологии и цели. Роль человеческого фактора.

4 Доктрина информационной безопасности РФ и последующие стратегические документы.

5 Понятие национальной безопасности. ИБ в системе национальной безопасности РФ. Информационный аспект в других составляющих национальной безопасности.

6 Основные источники угроз и угрозы ИБ РФ. Основные задачи по обеспечению ИБ РФ. Региональные проблемы информационной безопасности.

7 Модели информационного противоборства.

8 Законодательные акты в сфере информационной безопасности (ФЗ №149 от 27.07.2006, ФЗ №152 от 27.07.2006, Указ Президента №334 от 03.04.1995, Указ Президента РФ №351 от 17.03.2008, Постановление Правительства РФ №608 от 26.06.1995, №504 от 15.08.2006, №532 от 31.08.2006 и др.) и руководящие документы ФСБ РФ, ФСТЭК РФ, Роскомнадзора РФ.

9 Общеметодологические принципы теории ИБ. Стандарты и руководящие документы. Структура службы безопасности организации.

10 Принцип целенаправленности и целесообразности в анализе безопасности объектов и синтеза систем защиты.

11 Модели и методы риск анализа, основные представления, элементы и структура, факторы риска.

12 Методики расчета рисков.

13 Методика анализа и оценки рисков нарушения безопасности информационных объектов. ВИА. Непрерывность деятельности организации. ВСМ.

14 Оценка эффективности применения средств защиты. Соотношение надёжности и безопасности, допустимый ущерб.

15 Мониторинг и аудит безопасности, экспертные системы.

16 Физическая безопасность, методы и технические средства ее обеспечения.

Основные составляющие ИТСО.

- 17 Современные компьютерные методы обеспечения физической безопасности.
- 18 Нормативные документы в области ТСО. Оценка физической защищенности объекта информатизации.
- 19 Противодействие террористической деятельности в организации.
- 20 Требования Ф3187 (О безопасности КИИ...).
- 21 Требования Приказа ФСТЭК №31 (АСУ ТП).
- 22 Требования приказа ФСТЭК №235 (Требования к созданию систем безопасности значимых...).
- 23 Требования приказа ФСТЭК №239 (Требования по обеспечению безопасности...).
- 24 Международное взаимодействие с центрами мониторинга компьютерных воздействий.
- 25 Взаимодействие организации с ГосСОПКА.
- 26 НСД к информации, его место в проблеме информационной безопасности.
- 27 История международной нормативной базы в области ИБ.
- 28 РД ФСТЭК «Концепция защиты от НСД».
- 29 РД ФСТЭК «СВТ защита от НСД...»
- 30 РД ФСТЭК «АС защита от НСД...»
- 31 РД ФСТЭК «Защита от НСД. Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия не декларированных возможностей»
- 32 ГОСТ Р 15408 и его применение.
- 33 ГОСТы РФ в области ИБ.
- 34 Формальные модели информационной безопасности
- 35 Субъекты и объекты доступа к ресурсам, модели доступа. Правила разграничения доступа.
- 36 Понятие об идентификации и аутентификации субъектов доступа.
- 37 Классификация защищенности ГИС от НСД к информации.
- 38 Основные технические методы и средства получения НСД к информации.
- 39 Средства защиты информации от несанкционированного доступа (СЗИ от НСД).

АМДЗ

- 40 Единое информационное пространство РФ и методы его реализации.
- 41 Отечественные компьютеры на основе совместных технологий.
- 42 Отечественные компьютеры на основе российской аппаратной платформы.

Понятие защищенного компьютера.

- 43 Отечественное активное сетевое оборудование.
- 44 Реализация общероссийских защищенных компьютерных сетей.
- 45 Перспективы развития отечественных защищенных АС.
- 46 Оптические компьютеры и их применение.
- 47 Квантовые компьютерные технологии и их применение.
- 48 Информационная безопасность и перспективные технологии.
- 49 Механизмы защиты ОС. Отечественные защищенные ОС.
- 50 Механизмы защиты СУБД. Отечественные защищенные СУБД.