Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Дзержинский филиал ННГУ

УТВЕРЖДЕНО

решением Ученого совета ННГУ

протокол № 10 от 02.12.2024 г.

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования
Бакалавриат

Направление подготовки / специальность
09.03.03 - Прикладная информатика

Направленность образовательной программы
ИТ-сервисы и технологии обработки данных в экономике и финансах

Форма обучения
очно-заочная

г. Дзержинск

2025 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.21 Информационная безопасность относится к обязательной части образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**	
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
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-3.1: Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.* *ОПК-3.2: Демонстрирует умение применять информационно-коммуникационные технологии решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности* *ОПК-3.3: Имеет практический опыт решения стандартных задач профессиональной деятельности с соблюдением требований информационной безопасности.*	*ОПК-3.1:* *Знать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности* *Уметь использовать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности* *Владеть навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности* *ОПК-3.2:* *Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности*	*Собеседование* *Задания* *Тест*	*Экзамен:* *Задания* *Тест*

		Уметь *разработать требования по информационной безопасности для решения стандартных задач профессиональной деятельности* *Владеть* *навыками подбора и использования программно-технических средств для решения стандартных задач с учетом основных требований информационной безопасности* *ОПК-3.3:* *Знать* *принципы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности* *Уметь* *использовать основы информационной безопасности при подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе* *Владеть* *навыками использования методов и средств обеспечения информационной безопасности при подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе*		
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с	*ОПК-4.1: Демонстрирует знание основных стандартов, норм и правил оформления технической документации на различных стадиях проектирования и поддержки жизненного*	*ОПК-4.1:* *Знать* *основные законодательные акты в сфере информационной безопасности* *Уметь*	*Собеседование* *Задания* *Тест*	*Экзамен:* *Задания* *Тест*

профессиональной деятельностью;	*цикла информационных систем.* *ОПК-4.2: Применяет стандарты, нормы и правила (в том числе установленные самостоятельно) при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла информационных систем.* *ОПК-4.3: Имеет практический опыт разработки технической документации на различных этапах проектирования и поддержки жизненного цикла информационной системы.*	*использовать в практической деятельности существующие правовые знания в сфере информационных систем и информационных технологий* *Владеть навыками соблюдения норм и правил, существующих в виртуальной среде* *ОПК-4.2:* *Знать стандарты оформления технической документации с учетом информационной безопасности* *Уметь использовать стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом информационной безопасности* *Владеть навыками использования инструментов информационной безопасности при разработке технической документации* *ОПК-4.3:* *Знать основные инструменты информационной безопасности при составлении технической документации* *Уметь применять методы и средства информационной безопасности на различных этапах жизненного цикла ИС* *Владеть методами и средствами обеспечения информационной безопасности на различных этапах жизненного цикла информационной системы*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очно-заочная
Общая трудоемкость, з.е.	**4**
Часов по учебному плану	**144**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**12**
- занятия семинарского типа (практические занятия / лабораторные работы)	**12**
- КСР	**2**
самостоятельная работа	**82**
Промежуточная аттестация	**36** **Экзамен**

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)	в том числе			
		Контактная работа (работа во взаимодействии с преподавателем), часы из них			Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа (практические занятия/лабораторные работы), часы	Всего	
	о з ф о	о з ф о	о з ф о	о з ф о	о з ф о
Политика государства в области информационной безопасности	20	2	2	4	16
Угрозы и нарушители безопасности информации	24	4	4	8	16
Модель угроз безопасности информации	22	2	2	4	18
Политика безопасности организации	20	2	2	4	16
Системы обнаружения и предотвращения компьютерных атак	20	2	2	4	16
Аттестация	36				
КСР	2			2	
Итого	144	12	12	26	82

Содержание разделов и тем дисциплины

Тема 1. Политика государства в области информационной безопасности

Политика государства в области информационной безопасности. Угрозы и нарушители безопасности информации. Модель угроз безопасности информации. Политика безопасности организации. Системы обнаружения и предотвращения компьютерных атак. Основные стандарты в области информационной безопасности.

Тема 2. Угрозы и нарушители безопасности информации

Понятие угрозы безопасности информации. Виды угроз безопасности информации. Источники угроз

безопасности информации. Нарушители безопасности информации. Виды и цели нарушителей. Потенциал и возможности нарушителей. Способы реализации угроз нарушителем.
Тема 3. Модель угроз безопасности информации
Назначение модели угроз ИБ. Идентификация угроз безопасности информации и их источников. Модель нарушителя. Принцип оценки актуальности угроз. Оценка возможности реализации угрозы. Оценка степени ущерба. Оценка актуальности угрозы.
Тема 4. Политика безопасности организации
Понятие политики безопасности. Назначение и содержание политики безопасности. Вопросы, рассматриваемые в политике безопасности. Организационные аспекты информационной безопасности. Управление активами. Безопасность, связанная с управлением персоналом. Физическая безопасность. Управление доступом. Вопросы эксплуатации информационных систем. Управление инцидентами и непрерывностью бизнеса. Соответствие требованиям обязательств организации. Жизненный цикл политики безопасности.
Тема 5. Системы обнаружения и предотвращения компьютерных атак
Назначение систем обнаружения и предотвращения компьютерных атак. Понятие компьютерной атаки. Требования к системам обнаружения и предотвращения компьютерных атак. Классификация систем обнаружения и предотвращения компьютерных атак. Системы анализа защищенности. Системы обнаружения атак. Системы контроля целостности. Системы анализа журналов регистрации. Размещение систем обнаружения и предотвращения атак в информационной системе. Критерии выбора систем обнаружения и предотвращения компьютерных атак. Защита данных пользователя

Практическая часть
1. Работа со средствами криптографии
2. Шифры и криптоанализ
3. Защита бланка организации от редактирования средствами MS Word
4. Аппаратные системы безопасности ПК
5. Основы информационной и компьютерной безопасности
6. Настройки безопасности ОС типа Windows
7. Исследование стойкости системы идентификации, криптографии ОС типа Windows
8. Исследование программно-аппаратных средства анализа защищенности ОС типа Windows
9. Исследование уязвимости сетевой инфраструктуры с использованием сканеров безопасности Nessus и Nmap
10. Программно-аппаратные средства анализа безопасности передачи данных в локальных сетях

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Для обеспечения самостоятельной работы обучающихся используются:
Электронные курсы, созданные в системе электронного обучения ННГУ:

Информационная безопасность ПИ(Поляков Е.А.), https://e-learning.unn.ru/course/view.php?id=11693.

Иные учебно-методические материалы:
Теоретическая часть курса
Интерактивный курс:

Тестовые задания по всем темам курса.
Лекционный материал:
1. Политика государства в области информационной безопасности
2. Угрозы и нарушители безопасности информации
3. Модель угроз безопасности информации
4. Политика безопасности организации
5. Системы обнаружения и предотвращения компьютерных атак

Презентации:
Политика государства в области информационной безопасности
Угрозы и нарушители безопасности информации
Модель угроз безопасности информации
Политика безопасности организации
Системы обнаружения и предотвращения компьютерных атак

Лабораторный практикум
Практика 1. Работа со средствами криптографии
Практика 2. Шифры и криптоанализ
Практика 3. Защита бланка от редактирования средствами MS Word
Практика 4. Аппаратные системы безопасности ПК
Практика 5. Основы информационной и компьютерной безопасности
Практика 6. Первичные настройки безопасности ОС типа Windows
Практика 7. Исследование стойкости системы идентификации, криптографии ОС типа Windows
Практика 8. Исследование программно-аппаратных средства анализа защищенности ОС типа Windows
Практика 9. Исследование уязвимости сетевой инфраструктуры с использованием сканеров безопасности Nessus и Nmap
Практика 10. Программно-аппаратные средства анализа безопасности передачи данных в локальных сетях

Контроль по курсу
Экзаменационное занятие

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ОПК-3:

1. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
2. Дайте определение компьютерного вируса как саморепродуцирующейся программы?
3. Охарактеризуйте известные вам классы компьютерных вирусов.
4. Каковы должны быть основные правила работы с компьютером, предупреждающие возможное его заражение вирусами?
5. С чем, по вашему мнению, связана необходимость разработки нормативных документов по информационной безопасности?
6. Что такое государственная тайна?
7. Дайте определение средств защиты информации согласно Закону «О государственной тайне».
8. Сформулируйте основные положения Закона Российской Федерации «Об информации, информатизации и защите информации»
9. Сформулируйте цели защиты информации согласно Закону «Об информации, информатизации и защите информации».
10. Что такое оценочные стандарты и технические спецификации в области информационной безопасности?
11. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
12. Что такое монитор обращений?
13. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
14. Назовите основные способы аутентификации. Какой из этих способов является, по вашему мнению, наиболее эффективным?
15. Какие основные методы контроля доступа используются в современных автоматизированных системах?
16. Перечислите причины нарушения информационной безопасности в вычислительной сети.
17. Дайте определение понятию «технический канал утечки информации». Назовите основные виды этих каналов.

5.1.2 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ОПК-4:

1. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.
2. Дайте классификацию источников утечки информации
3. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.
4. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.
5. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.
6. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.
7. Дайте определение шифра и сформулируйте основные требования к нему.

8. Поясните, что вы понимаете под совершенным шифром? Приведите пример совершенного шифра.
9. Изложите принципиальную схему организации секретной связи с использованием системы шифрования с открытым ключом.
10. Изложите принципиальную схему организации обмена документами, заверенными цифровой подписью.
11. Почему действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы?
12. Сформулируйте основные концептуальные положения теории защиты информации.
13. Сформулируйте определение задачи защиты информации.
14. Приведите наиболее распространенные на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?
15. Раскройте содержание концепции управления системой защиты информации.
16. Раскройте содержание методологии создания, организации и обеспечения функционирования систем комплексной защиты информации.
17. Что такое сетевые сканеры безопасности и анализаторы протоколов?

Критерии оценивания (оценочное средство - Собеседование)

Оценка	Критерии оценивания
зачтено	Уровень знаний в объеме, соответствующем программе подготовки.
не зачтено	Уровень знаний ниже минимальных требований.

5.1.3 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-3:

1. Сколько уровней потенциала нарушителя выделяется в соответствии с методикой?

2. Какие защищенные поля документа могут быть использованы для подтверждения его юридической силы?
Для примера можно использовать функции любого текстового редактора.

3. В чем отличия защиты файлов в различных текстовых редакторах, включая облачные.
Для примера можно использовать функции любого текстового редактора, облачного сервиса.

4. Назовите способы защиты документа от несанкционированных действий пользователя.
Для примера можно использовать функции любого текстового редактора.

5. В каком году была разработана методика определения угроз информационной безопасности в информационных системах?

5.1.4 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-4:

1. Приведите порядок сброса пользовательского пароля в ОС типа Windows с использованием режима "Восстановление системы"
Перезагрузите компьютер:

- Нажмите и удерживайте клавишу **Shift**.
- Кликните "Пуск" (или "Меню питания") и выберите "Перезагрузка".

Войдите в режим восстановления:

- После перезагрузки компьютера, когда появится экран входа в систему, удерживайте клавишу **Shift** и одновременно щелкните "Пуск" (или "Меню питания") и выберите "ПЕРЕЗАГРУЗКА".
- После перезагрузки выберите "Устранение неполадок" ("Troubleshoot").

Выберите "Дополнительные параметры" ("Advanced options"):

- В меню "Устранение неполадок" выберите "Дополнительные параметры".

Выберите "Параметры загрузки" ("Startup Settings"):

- В "Дополнительных параметрах" найдите "Параметры загрузки" и выберите их.

Перезагрузите компьютер в режиме с отключенной проверкой цифровой подписи:

- После этого выберите "Перезагрузить" и, когда компьютер перезагрузится, нажмите клавишу **4** или **F4** для запуска в безопасном режиме с отключенной проверкой цифровой подписи.

Сбросьте пароль:

- После входа в систему с использованием безопасного режима, вы можете сбросить пароль в Управлении учетными записями.

2. Укажите порядок настройки любого браузера для повышения безопасности серфинга сайтов Интернет. Необходимо перечислить разделы и пользовательские настройки, кроме того указать примеры настройки встроенных инструментов, функций и дополнительных расширений.

Использование режима инкогнито:

- Режим инкогнито позволяет браузеру работать без сохранения истории, куки и данных форм. Он может быть включен в меню браузера (три точки в верхнем правом углу) -> "Новое окно инкогнито".

Обновление браузера:

- Важно всегда использовать последнюю версию браузера, чтобы иметь доступ к последним исправлениям безопасности. Обновление Chrome можно выполнить в разделе "Справка" -> "О Google Chrome".

Использование встроенных инструментов безопасности:

- Chrome предлагает встроенные инструменты безопасности, такие как "Блокировка сайтов" и "Защита от вредоносных программ". Они могут быть включены в настройках браузера.

Настройка параметров конфиденциальности и безопасности:

- Перейдите в "Настройки" -> "Дополнительные" -> "Конфиденциальность и безопасность". Здесь вы можете настроить параметры безопасности, включая управление куками, настройки контента и другие.

Использование расширений для повышения безопасности:

- Рассмотрите установку расширений, таких как HTTPS Everywhere, AdBlock, Privacy Badger и других, чтобы улучшить безопасность и анонимность в интернете.

Включение функции Safe Browsing:

- В "Настройках" -> "Дополнительные" -> "Конфиденциальность и безопасность" -> "Защита от вредоносных программ" убедитесь, что включена функция "Защита от вредоносных и опасных сайтов".

Очистка истории и данных браузера:

- Регулярно чистите историю, файлы cookie и кэш, особенно если вы используете общедоступные компьютеры. Это можно сделать в разделе "История" -> "Очистить данные браузера".

Использование виртуальной частной сети (VPN):

- Для дополнительного уровня анонимности можно рассмотреть возможность использования VPN, чтобы скрыть свой IP-адрес и шифровать интернет-соединение.

Настройка параметров поиска:

- Если используется поиск Google, удостоверьтесь, что настроены параметры конфиденциальности. Можно также рассмотреть использование поисковых систем, уделяющих больше внимания анонимности.

3. Приведите текст кода шаблонов учетной записи с использованием реестра:
Задача - зарегистрировать только один (пользовательский) USB-диск. При этом, отключить возможность чтения/записи любых других USB-накопителей.
В коде нужно указать расположение необходимого раздела и параметры ключа реестровой записи.

Замените 'X' на букву вашего USB-диска$allowedDriveLetter = 'X'# Создаем путь в реестре для USB-накопителей$registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies"# Проверяем наличие ключа WriteProtectif (-not (Test-Path $registryPath)) { # Если ключа нет, создаем его New-Item -Path $registryPath -Force | Out-Null}# Устанавливаем значение 1 для запрета записи на всех USB-накопителяхSet-ItemProperty -Path $registryPath -Name "WriteProtect" -Value 1# Создаем или обновляем ключ реестра для разрешения доступа к конкретному USB-диску$usbDiskRegistryPath = Join-Path $registryPath "ProviderProfiles\{4f69f170-b8b2-4a9e-9e62-2aa4f2b8ad89}"# Проверяем наличие ключа для USB-дискаif (-not (Test-Path $usbDiskRegistryPath)) { # Если ключа нет, создаем его New-Item -Path $usbDiskRegistryPath -Force | Out-Null}# Устанавливаем значение 0 для разрешения доступа только к конкретному USB-дискуSet-ItemProperty -Path $usbDiskRegistryPath -Name "$allowedDriveLetter:" -Value 0Write-Host "Доступ разрешен только для USB-диска с буквой $allowedDriveLetter."

4. Приведите текст кода шаблонов учетной записи с использованием реестра:
Задача - отключить установленную пользователем заставку экрана и снять пароль.
В коде нужно указать расположение необходимого раздела и параметры ключа реестровой записи.
Отключаем заставку экранаSet-ItemProperty -Path 'HKCU:\Control Panel\Desktop\' -Name ScreenSaveActive -Value 0# Снимаем пароль с аккаунта (замените 'ИмяПользователя' на фактическое имя пользователя)$Username = 'ИмяПользователя'$User = New-Object System.Security.Principal.NTAccount($Username)$UserSID = $User.Translate([System.Security.Principal.SecurityIdentifier]).Value# Получаем объект учетной записи пользователя$UserObj = Get-WmiObject -Class Win32_UserAccount | Where-Object { $_.SID -eq $UserSID }# Снимаем пароль$UserObj.SetPassword('')

5. Укажите порядок настройки ВСЕХ возможных элементов автозапуска в ОС типа Windows для исключения ненужных, удаленных или вредоносных процессов при запуске операционной системы.
Менеджер задач:

- Откройте "Менеджер задач" (нажмите Ctrl + Shift + Esc или правый клик на панели задачи и выберите "Менеджер задач").
- Перейдите на вкладку "Загрузка" (Startup).
- Здесь отображаются программы, запускающиеся вместе с системой. Вы можете отключить ненужные элементы, кликнув правой кнопкой мыши и выбрав "Отключить".

Системная конфигурация (msconfig):

- Нажмите Win + R, введите msconfig и нажмите Enter.
- Перейдите на вкладку "Службы" (Services).
- Убедитесь, что включен флажок "Скрыть все службы Microsoft".
- Отключите ненужные службы или службы, которые вам неизвестны.
- Перейдите на вкладку "Загрузка" (Startup) и отключите ненужные элементы.

Реестр Windows:

- Откройте "Редактор реестра" (regedit). Введите regedit в строке поиска и нажмите Enter.
- Перейдите к ключу реестра: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (для текущего пользователя) или HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (для всех пользователей).
- Здесь могут быть указаны программы, запускающиеся при старте. Вы можете удалить или отключить ненужные ключи.

Папки автозагрузки:

- Откройте папку автозагрузки, набрав shell:startup в строке поиска и нажав Enter. Это откроет папку автозагрузки текущего пользователя.
- Проверьте также папку C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup для автозагрузки всех пользователей.
- Удалите ярлыки ненужных программ или файлы, чтобы предотвратить их запуск.

Специальные программы для управления автозапуском:

- Используйте сторонние программы, такие как "CCleaner" или "Autoruns" от Microsoft Sysinternals, чтобы управлять элементами автозапуска более детально.

Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
зачтено	Уровень знаний в объеме, соответствующем программе подготовки.
не зачтено	Уровень знаний ниже минимальных требований.

5.1.5 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-3:

1. Сколько уровней реализации угроз существует?
Ответ:

_____

2. Расставьте логику осуществления угрозы безопасности информации:
1.
[1]_____
_____
2.
[2]_____
_____
3.
[3]_____
_____
4.
[4]_____
_____

A) Действие источника угрозы приводит к повреждению информации или информационной системы. B) Результатом угрозы является несанкционированный доступ. C) Угроза безопасности информации нацелена на действие.	D) Реализует используя некую уязвимость информационной системы. E) Источник угрозы информации реализует некое действие. F) Угроза безопасности информации имеет источник.

3. Кто является субъектом персональных данных в соответствии с законом о персональных данных?
A) Муниципальные органы власти

B) Юридические лица

C) Физические лица

D) Правоохранительные органы

4. Кто считается внешними антропогенными источниками угроз?
A) Криминальные структуры

B) Вспомогательный персонал

C) Охранники

D) Службы защиты информации

5. На что имеет право владелец информации, согласно «Об информации, информационных технологиях и о защите информации»?

A) Разрешение или ограничение доступа

B) Абсолютный контроль над информацией

C) Неограниченное распространение информации

D) Нарушение прав на неприкосновенность частной жизни

6. Что считается угрозами информационной безопасности?

A) Улучшение информации

B) Несанкционированный доступ

C) Удаление информации

D) Отрицание подлинности информации

E) Модификация информации

F) Уничтожение информации

7. Расположите следующие принципы в том порядке, в котором они представлены ФЗ «Об информации, информационных технологиях и о защите информации»:

A) _____ Недопустимость технологического фаворитизма

B) _____ Открытость информации

C) _____ Неприкосновенность частной жизни

D) _____ Равенство языков в информационных системах

8. Соотнесите тип злоумышленника с его описанием.

[1]	_____ Внутренние злоумышленники	A)	Лица с гостевым доступом
[2]	_____ Недобросовестные партнеры	B)	Сотрудники организации
[3]	_____ Персонал технологической поддержки	C)	Действуют извне информационной системы
[4]	_____ Внешние злоумышленники	D)	Лица с одноразовым авторизованным доступом

	E) Могут действовать из корыстных побуждений для получения конкурентных преимуществ

9. Какова основная цель режима коммерческой тайны, о которой говорится в законе?
A) Содействие общественному доступу

B) Прозрачность экономической деятельности

C) Увеличение доходов

D) Защита экологической информации

10. Справедливо ли это утверждение?
Понятие информационной сферы включает в себя как информацию, так и правовое регулирование соответствующих общественных отношений.
A) Да

B) Нет

5.1.6 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-4:

1. Актуальность угрозы, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., означает, что
A) существует актуальный для данной информационной системы нарушитель с достаточным потенциалом для реализации угрозы

B) в информационной системе существует достаточная вероятность реализации угрозы, а ее последствия имеют средний или высокий уровень наносимого ущерба

C) в информационной системе существует возможность реализации угрозы

D) реализация угрозы нанесет ущерб владельцу или оператору информации либо субъекту персональных данных

E) в информационной системе существует возможность реализации угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к нанесению ущерба

2. Укажите, какие процедуры относятся к управлению инцидентами ИБ?
A) передача расследования инцидента на более высокий уровень

B) определение источников угроз нарушений деятельности организации, оценка последствия таких угроз

C) уведомление об обязанностях по сообщению контактному лицу организации о любых инцидентах ИБ

D) обеспечение непрерывности деятельности организации, доступности информации на требуемом уровне

E) уведомление лиц, взаимодействующих с организацией, о процедурах информирования об

инцидентах

F) включение информационной безопасности в процесс управления непрерывностью деятельности организации

G) использование формальных процедур информирования об инцидентах

3. Укажите все обстоятельства, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., способные являться причиной техногенных угроз:

A) внедрение вредоносных элементов в аппаратное обеспечение или технические средства

B) низкое качество обслуживания со стороны обслуживающих лиц

C) отсутствие поддерживающей инфраструктуры или ее низкая эффективность

D) халатность со стороны лиц, обеспечивающих техническое обслуживание

E) низкое качество сетей связи или услуг связи

F) износ аппаратного обеспечения или технических средств

4. Укажите все действия, включаемые в процедуру инвентаризации активов:

A) сбор информации, необходимой для восстановления актива в случае инцидента

B) сбор информации для актуализации атрибутов и разрешений файлов актива

C) актуализация описи активов

D) назначение владельцев активов

E) определение уровней важности и необходимости обеспечения защиты активов

F) описание значимости активов

5. Укажите все основные задачи систем обнаружения и предотвращения компьютерных атак:

A) ликвидация необходимости в наличии высококвалифицированного персонала

B) автоматизация управления средствами защиты информации и их настройками

C) упрощение обработки значительных объемов информации

D) контроль действий пользователей ИС

E) контроль всех событий в системе

6. Что такое предположения безопасности?

A) в ней функционирует объект оценки

B) часть среды защиты

C) в ней функционирует защищаемый объект

D) часть описания среды

7. Укажите все процессы, при которых, согласно рекомендации по обеспечению соответствия требованиям обязательств организации, должны учитываться требования безопасности:

A) внедрение ИС

B) проектирование ИС

C) реализация ИС

D) функционирование ИС

E) использование ИС

8. Укажите общие типовые требования доверия безопасности:

A) поиск доверенного канала передачи

B) поиск доверенного маршрута

C) анализ стойкости функций безопасности

D) поиск разработчиком явных уязвимостей

E) независимое тестирование

F) анализ открытия сеанса с объектом оценки

G) контроль блокирования сеанса

H) контроль среды разработки

9. Сопоставьте принципы построения модели угроз информационной безопасности на основе методики ФСТЭК:

Моделирование угроз должно носить [1]_____ характер и осуществляться и на этапе проектирования информационной системы, и периодически в ходе эксплуатации.

Оценка угроз безопасности информации проводится [2]_____ методом.

A) временный	D) расчетным
B) периодический	E) систематический
C) проектным	F) экспертным

10. В рамках рассмотрения вопросов, посвященных управлению непрерывностью бизнеса, в политике безопасности организации следует сформулировать принципы

A) взаимосвязи информационной безопасности организации и процесса управления непрерывностью деятельностью организации

B) поддержки процесса управления непрерывностью деятельности организации мероприятиями в области информационной безопасности

C) активизации средств информационной безопасности в случае реализации угроз безопасности информации, направленных на нарушение непрерывности деятельности организации

D) включения информационной безопасности в процесс управления непрерывностью деятельности организации

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	75% и более правильных ответов
не зачтено	менее 75% правильных ответов

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**плохо**	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет.	Уровень знаний в объеме, превышающем программу подготовки.
Умения	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторым	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и	Продемонстрирован творческий подход к решению нестандартных задач

	ответа		и недочетами	недочетами		недочетов	

Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	**превосходно**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой
	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-3

Вариант 1

Задание 1. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

Задание 2. Сформулируйте основные концептуальные положения теории защиты информации.

Вариант 2.

Задание 1. Дайте определение средств защиты информации согласно Закону «О государственной тайне».

Задание 2. Раскройте необходимость разработки нормативных документов по информационной безопасности?

Вариант 3.

Задание 1. Раскройте содержание концепции управления системой защиты информации.

Задание 2. Изложите принципиальную схему организации обмена документами, заверенными цифровой подписью.

Вариант 4.

Задание 1. Что такое сетевые сканеры безопасности и анализаторы протоколов?

Задание 2. Дайте определение шифра и сформулируйте основные требования к нему.

Вариант 5.

Задание 1. Сформулируйте основные концептуальные положения теории защиты информации.

Задание 2. Сформулируйте определение задачи защиты информации.

Вариант 6.

Задание 1. Дайте классификацию источников утечки информации.

Задание 2. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

5.3.2 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-4

Код формируемой компетенции ОПК-4

Вариант 7.

Задание 1. Перечислите причины нарушения информационной безопасности в вычислительной сети.

Задание 2. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

Вариант 8.

Задание 1. Сформулируйте основные положения Закона Российской Федерации «Об информации, информатизации и защите информации»

Задание 2. Раскройте содержание методологии создания, организации и обеспечения функционирования систем комплексной защиты информации.

Вариант 9.

Задание 1. Дайте классификацию источников утечки информации.

Задание 2. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

Вариант 10.

Задание 1. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

Задание 2. Что такое монитор обращений?

Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
превосходно	не оценивается
отлично	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
очень хорошо	не оценивается
хорошо	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок
удовлетворительно	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.
неудовлетворительно	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.
плохо	не оценивается

5.3.3 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-3

1. Угроза безопасности информации, направленная на интересующую нарушителя ИС, с заранее известными ему характеристиками, называется, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г,

A) подготовленной

B) целенаправленной

C) адаптированной

D) избирательной

E) актуальной

2. Укажите все угрозы доступности информации:

A) искажение системного файла операционной системы, приводящее к невозможности ее запуска

B) внесение в исполняемый файл текста вируса

C) изменение оценки в электронном дневнике

D) вывод из строя USB носителя

E) отправка сетевых пакетов с поддельным адресом отправителя.

F) блокирование учетной записи пользователя в результате компьютерной атаки

3. В чем состоит суть Стратегии национальной безопасности РФ?

A) в ней определяются национальные интересы РФ

B) в ней определяются положение России в современном мире

C) определяются основные показатели состояния национальной безопасности

D) является базовым документом стратегического планирования

E) в ней определяются стратегические национальные приоритеты РФ

4. Основным рекомендациям по вопросам физической защиты, рассматриваемым в политике безопасности организации, соответствует ситуация, при которой

A) для всего объекта информатизации обеспечивается единый уровень защищенности, не имеющий более слабых мест.

B) вся информация организации размещается таким образом, чтобы находиться в наиболее удобных для доступа персонала зонах, в непосредственной близости от рабочих мест пользователей

C) для повышения удобства пользователей контроль доступа осуществляется только при непосредственном входе на территорию объекта информатизации

D) уровень защищенности всего объекта в целом и его отдельных зон устанавливается в зависимости от выявленных рисков информационной безопасности

5. Какие угрозы существуют в классе по компонентам объекта информатизации?

A) нарушение целостности

B) воздействие на данные

C) нарушение конфиденциальности

D) воздействие на программы

E) нарушение доступности

F) воздействие на аппаратуру

6. Укажите цель построения угроз информационной безопасности ИС:

A) будет ли нанесен ущерб трем обладателям информации

B) существует ли вероятность нарушения работы информационной системы

C) есть ли возможность нарушения безопасности информации

D) будет ли угроза нанесения ущерба трем обладателям информации

E) будет ли нанесен ущерб операторам информационной системы

7. Что такое предположения безопасности?

A) часть описания среды

B) в ней функционирует объект оценки

C) часть среды защиты

D) в ней функционирует защищаемый объект

5.3.4 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-4

8. Что такое национальная безопасность Российской Федерации?

Это состояние защищенности [1]_____,
[2]_____ и
[3]_____ от внутренних и внешних угроз, при котором обеспечиваются реализация
[4]_____ граждан Российской Федерации (далее - граждане),
[5]_____, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации.

A) общества	F) обеспечение защищенности
B) приоритеты финансирования государственных программ	G) государства
C) борьба с терроризмом и экстремизмом	H) борьба с коррупцией
D) личности	I) достойные качество и уровень их жизни

E) конституционных прав и свобод	

9. Что такое свобода выражения мнения с точки зрения информационной безопасности России?

A) право человека свободно распространять информацию и идеи без какого-либо ограничения

B) право выполнять Конституцию РФ, федеральные законы и иные законодательные и исполнительные акты в части свободы распространения информации

C) право человека свободно выражать и придерживаться своего мнения

D) обязанность выполнять Конституцию РФ, федеральные законы и иные законодательные и исполнительные акты в части свободы распространения информации

10. К какому разделу ИБ организации относятся мероприятия по размещению важной информации в зонах безопасности, оборудованных средствами контроля доступа и соответствующими защитными средствами?

A) управление активами

B) физическая безопасность

C) безопасность управления персоналом

D) мандатная модель управления доступом

E) управление инцидентами и непрерывностью бизнеса

11. Укажите все основные задачи систем обнаружения и предотвращения компьютерных атак:

A) контроль всех событий в системе

B) упрощение обработки значительных объемов информации

C) ликвидация необходимости в наличии высококвалифицированного персонала

D) автоматизация управления средствами защиты информации и их настройками

E) контроль действий пользователей ИС

12. Актуальность угрозы, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., означает, что

A) в информационной системе существует возможность реализации угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к нанесению ущерба

B) реализация угрозы нанесет ущерб владельцу или оператору информации либо субъекту персональных данных

C) существует актуальный для данной информационной системы нарушитель с достаточным потенциалом для реализации угрозы

D) в информационной системе существует возможность реализации угрозы

E) в информационной системе существует достаточная вероятность реализации угрозы, а ее последствия имеют средний или высокий уровень наносимого ущерба

13. Что содержит модель нарушителя?

A) возможные цели и потенциал нарушителей

B) возможные способы реализации угроз безопасности информации

C) актуальные угрозы информационной безопасности

D) типы и виды нарушителей

E) условия построения модели нарушителей

F) описание ИС и ее особенностей

14. Сопоставьте понятия ИБ и их определения:

[1]_____ — это совокупность мер, регламентирующих повседневную жизнь организации

[2]_____ — это система, направленная на обнаружение нарушений и повседневного функционирования объекта информатизации

A) система аудита и контроля B) политика безопасности	C) система обнаружения атак

15. Укажите только общие предположения безопасности из перечисленных:

A) обход злоумышленником защитных средств

B) маскарад пользователя

C) осуществление злоумышленником физического доступа к вычислительной установке

D) не допускается возможность обхода узлов сети, на которых функционируют сервисы безопасности

E) возможность удаленного администрирования сервиса

F) резервное копирование информации, ассоциированной с сервисом

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
превосходно	не оценивается

Оценка	Критерии оценивания
отлично	>95% правильных ответов
очень хорошо	не оценивается
хорошо	>85 до 95% правильных ответов
удовлетворительно	>75 до 85% правильных ответов
неудовлетворительно	менее 75% правильных ответов
плохо	не оценивается

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Ворона А. А. Информационно-экономическая и информационная безопасность в условиях функционирования центров электронного декларирования : учебное пособие / Ворона А. А.,Коптева Л. А. - 2-е изд., доп. - Санкт-Петербург : Интермедия, 2022. - 182 с. - Книга из коллекции Интермедия - Информатика. - ISBN 978-5-4383-0246-9., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=881457&idb=0.
2. Зенков А. В. Информационная безопасность и защита информации : учебное пособие / А. В. Зенков. - 2-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 107 с. - (Высшее образование). - ISBN 978-5-534-16388-9. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=871683&idb=0.
3. Никулин В. В. Информационная безопасность. Лабораторный практикум : учебно-методическое пособие для студентов направления подготовки 09.03.03 прикладная информатика / Никулин В. В. - Брянск : Брянский ГАУ, 2021. - 84 с. - Книга из коллекции Брянский ГАУ - Информатика., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=860117&idb=0.

Дополнительная литература:

1. Информационная безопасность и защита информации : практикум / Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. - Дубна : Государственный университет «Дубна», 2020. - 85 с. - Рекомендовано учебно-методическим советом университета «Дубна» в качестве практикума для студентов, обучающихся по направлениям подготовки «Системный анализ и управление», «Прикладная информатика», «Прикладная математика и информатика (магистратура). - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции Государственный университет «Дубна» - Информатика. - ISBN 978-5-89847-608-3., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=730800&idb=0.
2. Стрижакова Е. А. Информационная безопасность в профессиональной деятельности: лабораторный практикум для обучающихся по специальности 38.05.01 Экономическая безопасность / Стрижакова Е. А.,Пенькова Р. И. - Волгоград : Волгоградский ГАУ, 2022. - 92 с. -

Книга из коллекции Волгоградский ГАУ - Информатика., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=866608&idb=0.
3. Басыня Е. А. Сетевая информационная безопасность : учебник / Басыня Е. А. - Москва : НИЯУ МИФИ, 2023. - 224 с. - Книга из коллекции НИЯУ МИФИ - Информатика. - ISBN 978-5-7262-2949-2., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=884189&idb=0.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

1. Операционная система Microsoft Windows
2. Пакет прикладных программ Microsoft Office

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки/специальности 09.03.03 - Прикладная информатика.

Автор(ы): Поляков Евгений Артурович, кандидат педагогических наук.

Заведующий кафедрой: Поляков Евгений Артурович, кандидат педагогических наук.

Программа одобрена на заседании методической комиссии от 28.12.2024, протокол № 21.