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 от «14» декабря 2021 г. № 4)

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Направленность (профиль) образовательной программы

ИТ-СЕРВИСЫ И ТЕХНОЛОГИИ ОБРАБОТКИ ДАННЫХ В ЭКОНОМИКЕ И ФИНАНСАХ

Год набора: 2021

Квалификация

БАКАЛАВР

Форма обучения

ОЧНАЯ

Дзержинск
2021 г.

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.21 Информационная безопасность относится к обязательной части учебного плана ООП 09.03.03 Прикладная информатика.

Целями освоения дисциплины являются:

- изучение принципов обеспечения информационной безопасности, подходов к анализу угроз информационной инфраструктуры организации;
- освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах.

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**	
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. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	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	доклады, тестирование, практические задания
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности 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	доклады, тестирование, практические задания
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по	Знать принципы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности Уметь	доклады, тестирование, практические задания

	научно-исследовательской работе с учетом требований информационной безопасности.	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 профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знать основные законодательные акты в сфере информационной безопасности Уметь использовать в практической деятельности существующие правовые знания в сфере информационных систем и информационных технологий Владеть навыками соблюдения норм и правил, существующих в виртуальной среде	доклады, тестирование, практические задания
	ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	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	доклады, тестирование, практические задания
	ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	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	доклады, тестирование, практические задания

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	**Очно**-заочная **форма обучения**

Общая трудоемкость	4 ЗЕТ	4 ЗЕТ
Часов по учебному плану	144	144
в том числе		
аудиторные занятия (контактная работа): **- занятия лекционного типа** **- занятия семинарского типа** **- кср**	50 16 32 2	32 10 20 2
самостоятельная работа	58	76
Промежуточная аттестация – экзамен	36	36

3.2. Содержание дисциплины

Наименование и краткое содержание 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**			**Занятия лабораторного типа**			**Всего**					
	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная
1. Политика государства в области информационной безопасности	18			2			6						8			10		
2. Угрозы и нарушители безопасности информации	22			4			6						10			12		
3. Модель угроз безопасности информации	20			2			6						8			12		
4. Политика безопасности организации	22			4			8						12			10		
5. Системы обнаружения и предотвращения компьютерных атак	24			4			6						10			14		
КСР	2												2					

Промежуточная аттестация	36																	
Итого	144			16			32						50			58		

Практическая подготовка предусматривает: – выполнение проекта по профилю профессиональной деятельности и направленности образовательной программы.

На проведение практических занятий (семинарских занятий /лабораторных работ) в форме практической подготовки отводится _20___ часов.

Практическая подготовка направлена на формирование и развитие:

- практических навыков в соответствии с профилем ОП:

• Составление технико-экономического обоснования проектных решений и технического задания на разработку информационной системы

• Участие в организации работ по управлению проектами информационных систем

• Информационное обеспечение прикладных процессов.

- компетенций - 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;

- компетенций - ОПК-4

Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

Текущий контроль успеваемости реализуется в рамках занятий лабораторного типа.

Промежуточная аттестация проходит в традиционной форме - зачет, включающий ответы на вопросы по программе дисциплины.

Содержание дисциплины по темам

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

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа проводится с целью углубления знаний по дисциплине и предусматривает:

1. Работу с компьютерными обучающими программами, электронными учебниками, лабораторными практикумами, тестовыми системами.
2. Использование профессиональных прикладных программ.
3. Использование средств телекоммуникаций, в том числе электронной почты, участие в видеоконференциях, форумах по курсу.
4. Работу с электронными библиотеками, распределенными издательскими системами.
5. Подготовку докладов и презентационных материалов.
6. Электронное обучение с использованием Интернет.
7. Повторение пройденного учебного материала, чтение рекомендованной литературы;
8. Подготовку к практическим занятиям;
9. Выполнение общих и индивидуальных заданий;
10. Работу с Интернет и прочими электронными источниками;
11. Подготовку к сдаче зачета.

Планирование времени на самостоятельную работу важно осуществлять на весь семестр, предусматривая при этом повторение пройденного материала.

Самостоятельная работа студентов, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

Предполагается, что, прослушав лекцию, студент должен ознакомиться с рекомендованной литературой из основного списка, затем обратится к источникам, указанным в библиографических списках изученных книг, осуществит поиск и критическую оценку материала на сайтах Интернет, соберет необходимую информацию.

Существует несколько методов работы с литературой.

Один из них – *метод повторения*: смысл прочитанного текста можно заучить наизусть. Простое повторение воздействует на память механически и поверхностно. Полученные таким путем сведения легко забываются.

Наиболее эффективный метод – *метод осознанного запоминания*: прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке. Чтобы основательно обработать информацию, важно произвести целый ряд мыслительных операций: прокомментировать новые данные; оценить их значение; поставить вопросы; сопоставить полученные сведения с ранее известными.

Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения. Изучение научной, учебной и иной литературы требует ведения рабочих записей. Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

При *подготовке к промежуточной аттестации по дисциплине* следует руководствоваться перечнем вопросов для подготовки к **зачету** по курсу.

Практические занятия (семинарские занятия /лабораторные работы) организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

Для обеспечения самостоятельной работы обучающихся используется электронный курс Информационная безопасность (https://e-learning.unn.ru/course/view.php?id=2193), созданный в системе электронного обучения ННГУ - https://e-learning.unn.ru/

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), включающий:

5.1.Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	**Шкала оценивания сформированности компетенций**						
	плохо	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	Не зачтено		зачтено				
Знания	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественн	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу

	вследствие отказа обучающегося от ответа			ошибок	ых ошибок		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 несущественным 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 владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	Превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно»
	Отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	Очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»
	Хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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», ни одна из компетенций не сформирована на уровне «плохо»
	Плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1 Контрольные вопросы (код формируемых компетенций ОПК-3, ОПК-4)

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.
18. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.
19. Дайте классификацию источников утечки информации

20. Охарактеризуйте методы контроля информации техническими средствами в каналах телефонной связи.

21. Назовите методы контроля информации, обрабатываемой средствами вычислительной техники.

22. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

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

24. Дайте определение шифра и сформулируйте основные требования к нему.

25. Поясните, что вы понимаете под совершенным шифром? Приведите пример совершенного шифра.

26. Изложите принципиальную схему организации секретной связи с использованием системы шифрования с открытым ключом.

27. Изложите принципиальную схему организации обмена документами, заверенными цифровой подписью.

28. Почему действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы?

29. Сформулируйте основные концептуальные положения теории защиты информации.

30. Сформулируйте определение задачи защиты информации.

31. Приведите наиболее распространенные на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

32. Раскройте содержание концепции управления системой защиты информации.

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

34. Что такое сетевые сканеры безопасности и анализаторы протоколов?

5.2.2. Типовые тестовые задания для оценки сформированности компетенции

Тесты для проверки компетенции ОПК-3, ОПК-4

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

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	C) система обнаружения атак
B) политика безопасности	

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

5.2.3. Типовые задания/задачи для оценки сформированности компетенции ОПК-3, ОПК-4

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.
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?

5.2.4. Темы докладов

Темы для докладов-презентаций

1. Актуальность проблемы обеспечения безопасности информационных технологий
2. Информация и информационные отношения. Субъекты информационных отношений, их безопасность
3. Свойства информации и систем ее обработки
4. Цель защиты автоматизированной системы и циркулирующей в ней информации
5. Особенности современных автоматизированных систем как объекта защиты
6. Уязвимость основных структурно-функциональных элементов распределенных систем
7. Источники угроз безопасности и их классификация
8. Классификация каналов проникновения в систему и утечки информации
9. Меры защиты информации
10. Достоинства и недостатки различных видов мер защиты
11. Основные принципы построения системы защиты
12. Основные механизмы защиты компьютерных систем
13. Криптографические методы защиты
14. Задачи, решаемые средствами защиты информации от несанкционированного доступа
15. Проблемы обеспечения безопасности в IP-сетях
16. Уязвимость IP-сетей
17. Межсетевые экраны
18. Типы межсетевых экранов
19. Механизмы трансляции сетевых адресов
20. Виртуальные частные сети (Virtual Private Networks - VPN)

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М.: Издательство Юрайт, 2017. — 312 с. — (Серия: Специалист). — ISBN 978-5-9916-9043-0. (доступно в ЭБС «Юрайт», режим доступа https://urait.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-452368)[Дата обращения: 23.04.2020]

2. Внуков, А. А. Защита информации: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М.: ИздательствоЮрайт, 2017. — 261 с. — (Серия: Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. (доступно в ЭБС «Юрайт», режим доступа https://urait.ru/viewer/zaschita-informacii-v-bankovskih-sistemah-414083 Дата обращения: 23.04.2020]

3. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. — М.: Издательство Юрайт, 2017. — 325 с. — (Серия: Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. (доступно в ЭБС «Юрайт», режим доступа https://urait.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-450371)[Дата обращения: 23.04.2020]

4. Поляков Е.А. Интерактивный курс Информационная безопасность бакалавриата / Поляков Е.А. - Электрон. текстовые данные, обучающий курс — ДФ ННГУ, 2020. — Режим доступа: https://e-learning.unn.ru/course/view.php?id=2193 — ИОС ННГУ им. Лобачевского

б) дополнительная литература:

1. Гришина, Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - Москва : Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; . - (Высшее образование: Бакалавриат). ISBN 978-5-00091-007-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/491597 (дата обращения: 23.04.2020). – Режим доступа: по подписке]

2. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/reader/book/125739/#1 (дата обращения: 23.04.2020). — Режим доступа: для авториз. пользователей.

3. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 23.04.2020). — Режим доступа: для авториз. пользователей.

4. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - Москва : НИЦ ИНФРА-М, 2016. - 118 с. (Высшее образование: Бакалавриат) ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/507334 (дата обращения: 23.04.2020). – Режим доступа: по подписке.

в) программное обеспечение и Интернет-ресурсы

1. http://all-ib.ru/Информаицонная безопасность

2. http://securitypolicy.ru/index.php/Документы по информационной безопасности
3. Операционная системаMicrosoftWindows
4. Пакет прикладных программ MicrosoftOffice
5. Правовая система «Консультант плюс»
6. Правовая система «Гарант».

7. Материально-техническое обеспечение дисциплины

Реализация программы предполагает наличие:

- аудиторий для лекционных и практических занятий с необходимым оборудованием;
- компьютерного класса, имеющего компьютеры, объединенные сетью с выходом в Интернет;
- лицензионного (операционная система MicrosoftWindows, пакет прикладных программ MicrosoftOffice) и свободно распространяемого программного обеспечения.
- интернетбраузеров (Mozilla Firefox, Google Chrome, Safari, Opera),
- свободного пакета офисных приложений OpenOffice.

В ходе проведения занятий рекомендуется использовать компьютерные иллюстрации для поддержки различных видов занятий, подготовленные с использованием MicrosoftOffice или других средств визуализации материала.

Доступ к электронным информационным ресурсам осуществляется в компьютерном классе и библиотеке филиала.

Специальные условия организации обучения по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

Организация обучения по дисциплине инвалидов и лиц с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья при наличии таких обучающихся путем создания специальных условий для получения образования.

Профессорско-преподавательский состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии).

В соответствии с Методическими рекомендациями по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утв. Минобрнауки РФ 08.04.2014 АК-44/05вн при изучении дисциплины предполагается использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При освоении дисциплины используются различные сочетания видов учебной работы с методами и формами активизации познавательной деятельности обучающихся для достижения запланированных результатов обучения и формирования компетенций. Форма проведения промежуточной аттестации для обучающихся-инвалидов и лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизиологических особенностей. По личной просьбе обучающегося с ограниченными возможностями здоровья, изложенной в форме письменного заявления, по дисциплине предусматриваются:

- замена устного ответа на письменный ответ при сдаче зачета или зачета;
- увеличение продолжительности времени на подготовку к ответу на зачете;
- при подведении результатов промежуточной аттестации студентов выставляется максимальное количество баллов за посещаемость аудиторных занятий.

Программа составлена в соответствии с требованиями ФГОС ВО/ОС ННГУ по направлению 09.03.03 Прикладная информатика (приказ №349-ОД от 21.06.2021).

Автор(ы): к.п.н. доцент Поляков Е.А.

Рецензент:

Программа одобрена на заседании Методической комиссии Дзержинского филиала ННГУ, протокол № 4 от 07.06.2021 года.