МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ:
Проректор по образовательной деятельности,
председатель методического совета
_____ Д.В. Терентьев
9 февраля 2022 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

*УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ*

**Для основных образовательных программ**
**с индивидуальной образовательной траекторией**

Уровень высшего образования – бакалавриат

Форма обучения
Очная

Курс 4
Семестр 7

Магнитогорск
2022 г.

Рабочая программа рассмотрена и одобрена на заседании методического совета 09.02.2022, протокол № 1.

Согласовано с руководителями ООП:

| | |
|---|---|
| Зав. кафедрой ЭПП | А.В. Варганова |
| Зав. кафедрой экономики | А.Г. Васильева |
| Директор ИЕиС, зав. кафедрой ТССА | И.Ю. Мезин |
| Доцент кафедры ПОиД | Т.Г. Перетина |
| Зав. кафедрой УиИС | М.М. Суровцов |
| Зав. кафедрой ЛПиМ | Н.А. Фсоктистов |
| Доцент кафедры ЛиУТС | О.В. Фридрихсон |
| Зав. кафедрой МиХТ | А.С. Харченко |

**1 Цели освоения дисциплины (модуля)**

1) определение и оценка угроз, разработка моделей угроз в ходе создания и эксплуатации информационных систем;

2) выявление, анализ и устранение уязвимостей в ходе создания и эксплуатации

3) выявление источников угроз несанкционированного доступа (НСД)

4) определение типа нарушителя

**2 Место дисциплины (модуля) в структуре образовательной программы**

Дисциплина Угрозы кибербезопасности входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Цифровая грамотность

Персональная эффективность

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Проектная деятельность

**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**

В результате освоения дисциплины (модуля) «Угрозы кибербезопасности» обучающийся должен обладать следующими компетенциями:

| Код индикатора | Индикатор достижения компетенции |
|---|---|
| ДПК-004-5 Способен обеспечить функционирование средств защиты информации в информационно-аналитических системах | |
| ДПК-004-5.1 | Применяет знания в области безопасности вычислительных сетей в информационных системах |
| ДПК-004-5.2 | Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах |

**4. Структура, объём и содержание дисциплины (модуля)**

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 28,1 акад. часов:

– аудиторная – 28 акад. часов;

– внеаудиторная – 0,1 акад. часов;

– самостоятельная работа – 79,9 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

| Раздел/ тема дисциплины | Семестр | Аудиторная контактная работа (в акад. часах) | | | Самостоятельная работа студента | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код компетенции |
|---|---|---|---|---|---|---|---|---|
| | | Лек. | лаб. зан. | практ. зан. | | | | |
| 1. Нормативные и правовые акты в области защиты информации | | | | | | | | |
| 1.1 Основные понятия и задачи моделирования угроз кибербезопасности. База данных угроз ФСТЭК РФ. | 7 | | | 2 | 2 | Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме. | Текущий контроль успеваемости: – устный опрос (собеседование); – семинарские занятия; | ДПК-004-5.2 |
| Итого по разделу | | | | 2 | 2 | | | |
| 2. Этапы моделирования угроз ИБ | | | | | | | | |
| 2.1 Выявление объектов информационной системы, подлежащих защите. Определение источников угроз | 7 | | | 2 | 6 | Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме | Текущий контроль успеваемости: – контрольные работы; – проверка индивидуальных заданий | ДПК-004-5.1, ДПК-004-5.2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2 Наиболее часто реализуемые угрозы. Выявление способов реализации угроз | | | | 4 | 20 | Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме | Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – проверка индивидуальных заданий | ДПК-004-5.1, ДПК-004-5.2 |
| 2.3 Угрозы мобильным устройствам. | | | | 4 | 10,9 | Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме | Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий | ДПК-004-5.1, ДПК-004-5.2 |
| Итого по разделу | | | | 10 | 36,9 | | | |
| 3. Модель угроз ИСПДн информационной системы персональных данных | | | | | | | | |
| 3.1 Угрозы безопасности ПДн. Каналы реализации угроз безопасности ПДн. | 7 | | | 8 | 20 | Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме | Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий | ДПК-004-5.1, ДПК-004-5.2 |
| 3.2 Классификация угроз безопасности персональных данных по способу реализации | | | | 4 | 10 | Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме | Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий | ДПК-004-5.1, ДПК-004-5.2 |
| Итого по разделу | | | | 12 | 30 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4. Методики построение дерева угроз | | | | | | | | |
| 4.1 Разработка модели информационной безопасности с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании | 7 | | | 4 | 11 | Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме | Текущий контроль успеваемости: – проверка индивидуальных заданий | ДПК-004-5.1, ДПК-004-5.2 |
| Итого по разделу | | | | 4 | 11 | | | |
| Итого за семестр | | | | 28 | 79,9 | | зачёт | |
| Итого по дисциплине | | | | 28 | 79,9 | | зачет | |

**5 Образовательные технологии**

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. 2) Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. 3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. 4) Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. 5) Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. 6) Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания.

Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. 7) Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

**6 Учебно-методическое обеспечение самостоятельной работы обучающихся**

Представлено в приложении 1.

**7 Оценочные средства для проведения промежуточной аттестации**

Представлены в приложении 2.

**8 Учебно-методическое и информационное обеспечение дисциплины (модуля)**

**а) Основная литература:**

1. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект*. - ISBN 978-5-9967-1031-7

2. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 20.01.2023)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .

2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)

3. Активизировать гиперссылку макрообъекта.

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты

**б) Дополнительная литература:**

1. Модель угроз ПД. : Организационно-распорядительная документация по защите ПД [Электронный ресурс]. Национальный открытый университет «Интуит»/.- Режим доступа: http://www.intuit.ru/studies/courses/697/553/lecture2447.- Заглавие с экрана.

2. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 20.01.2023)

**в) Методические указания:**

1. Методические указания по выполнению практических работ. (Приложение 3.)

2. Методические указания по выполнению внеаудиторных самостоятельных работ. (Приложение 4.)

**г) Программное обеспечение и Интернет-ресурсы:**

**Программное обеспечение**

| Наименование ПО | № договора | Срок действия лицензии |
|---|---|---|
| MS Office 2007 | № 135 от 17.09.2007 | бессрочно |
| 7Zip | свободно | бессрочно |
| LibreOffice | свободно | бессрочно |
| MS Office 2003 | № 135 от 17.09.2007 | бессрочно |
| FAR Manager | свободно | бессрочно |
| Linux | свободно | бессрочно |

**Профессиональные базы данных и информационные справочные системы**

| Название курса | Ссылка |
|---|---|
| Информационная система - Банк данных угроз | https://bdu.fstec.ru/ |
| Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и | https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii |
| Национальная информационно-аналитическая система – Российский индекс | URL: https://elibrary.ru/project_risc.asp |
| Поисковая система Академия Google (Google Scholar) | URL: https://scholar.google.ru/ |

**9 Материально-техническое обеспечение дисциплины (модуля)**

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для самостоятельной работы обучающихся:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

# УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

**Темы практических работ**

1. Цели и задачи моделирования угроз ИБ
2. Нормативная база предметной области
3. Этапы моделирования угроз ИБ.
4. Описание структуры ИС,состав ИС, взаимосвязи между сегментами ИС, взаимосвязи с другими ИС и ИТКС, и условия функционирования ИС
5. Способы реализации угроз
6. Разработка мер по защите ИС. Базовый набор мер;-адаптированный базовый набор мер; -уточненный адаптированный базовый набор мер
7. Оценка материального ущерба и других последствий возможной реализации угроз, ранжирование угроз по потенциальному ущербу
8. . Формирование перечня активов, определение их значимости для компании.
9. Составление модели нарушителя, типы нарушителей, категории нарушителей
10. Построение дерева угроз.
11. Источники угроз ИБ. Классификация источников угроз
12. Классификация нарушителей
13. Оценка возможностей нарушителей
14. Потенциал нарушителя ИБ
15. Актуальные угрозы безопасности
16. Оценка степени ущерба
17. Структура модели угроз

Индивидуальное задание «Составление модели угроз для объекта информатизации»

- Определить перечень защищаемых ресурсов, состав персонала и категории доступа
- Определить класс (уровень защищенности от НСД) согласно РД ФСТЭК
- Определить угрозы безопасности информации на защищаемом объекте (Использовать Банк данных угроз безопасности информации)
- Определение «Угроза безопасности Пдн»
- Реализация угроз безопасности Пдн
- Источники угроз
- Определение «Нарушитель»
- Классификация нарушителей
- Порядок определения исходной степени защищенности
- Понятие «Частота (вероятность) реализации угрозы»

Оценка ущерба от реализации угрозы

ПРИЛОЖЕНИЕ 2

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

**а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:**

| Код индикатора | Индикатор достижения компетенции | Оценочные средства |
|---|---|---|
| ДПК-004-5 Способен обеспечить функционирование средств защиты информации в информационно-аналитических системах | | |
| ДПК-004-5.1 | Применяет знания в области безопасности вычислительных сетей в информационных системах | 1. Определить источники угроз для объекта информатизации.<br>2. Сформировать список уязвимостей выбранного объекта защиты, которые могут быть использованы для реализации угроз.<br>3. Определить перечень угроз безопасности выбранного объекта на основе имеющихся отечественных каталогов угроз. |
| ДПК-004-5.2 | Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах | 1. Средства моделирования угроз.<br>2. Составить модель угроз ПДн согласно методическому документу «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021).<br>3. Построить дерево угроз ИС.<br>4. Составить модель нарушителя. |

**б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:**

**Показатели и критерии оценивания зачета:**

– на **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.