САМАРСКИЙ ПОЛИТЕХ
Самарский университет

**МИНОБРНАУКИ РОССИИ**
федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Самарский государственный технический университет»**
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Директор филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
_____ / Г.И. Заболотни
"_____" _____ 20___ г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## ФТД.02 «Основы информационной безопасности»

| | |
|---|---|
| **Код и направление подготовки (специальность)** | 13.03.02 Электроэнергетика и электротехника |
| **Направленность (профиль)** | Электроэнергетика |
| **Квалификация** | Бакалавр |
| **Форма обучения** | Очная |
| **Год начала подготовки** | 2020 |
| **Институт / факультет** | Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске |
| **Выпускающая кафедра** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Кафедра-разработчик** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Объем дисциплины, ч. / з.е.** | 72 / 2 |
| **Форма контроля (промежуточная аттестация)** | Зачет |

Самара 2020

**ФТД.02 «Основы информационной безопасности»**

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **13.03.02 Электроэнергетика и электротехника**, утвержденного приказом Министерства образования и науки РФ от № 144 от 28.02.2018 и соответствующего учебного плана.

Разработчик РПД:

| | |
|---|---|
| Старший преподаватель | С.П Минеев |
| (должность, степень, ученое звание) | (ФИО) |

| | |
|---|---|
| Заведующий кафедрой | Е.М. Шишков, кандидат технических наук, доцент |
| | (ФИО, степень, ученое звание) |

## СОГЛАСОВАНО:

| | |
|---|---|
| Председатель методического совета факультета / института (или учебно-методической комиссии) | Н.А Сухова |
| | (ФИО, степень, ученое звание) |
| Руководитель образовательной программы | Е.М. Шишков, кандидат технических наук, доцент |
| | (ФИО, степень, ученое звание) |

Содержание

## 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Наименование категории (группы) компетенций | Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции) |
|---|---|---|---|
| Универсальные компетенции | | | |
| Безопасность жизнедеятельности | УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуация и военных конфликтов | УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций | Владеть инструментами и методами защиты информации; механизмами реакции на инциденты; навыком распознавания заражений и точечных атак, действий хакеров; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. |
| | | | Знать основные концепции кибербезопасности; типы угроз; основные тренды в области защиты информации; методы и способы защиты от существующих угроз и кибератак; содержание информационной войны, методы и средства ее ведения; современные подходы к построению систем защиты информации; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; |

| | | | |
|---|---|---|---|
| | | | Уметь идентифицировать существующие и потенциальные риски; оценивать качество защиты данных; корректно и оперативно реагировать на инциденты безопасности; выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; |

## 2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **блок факультативных дисциплин**

| Код компетенции | Предшествующие дисциплины | Параллельно осваиваемые дисциплины | Последующие дисциплины |
|---|---|---|---|
| УК-8 | Безопасность жизнедеятельности; Производственная практика: проектная практика; Учебная практика: профилирующая практика | Государственная итоговая аттестация: подготовка к процедуре защиты и защита выпускной квалификационной работы; Производственная практика: преддипломная практика | |

## 3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

| Вид учебной работы | Всего часов / часов в электронной форме | 8 семестр часов / часов в электронной форме |
|---|---|---|
| **Аудиторная контактная работа (всего),** в том числе: | 32 | 32 |
| Лекции | 16 | 16 |
| Практические занятия | 16 | 16 |
| **Самостоятельная работа (всего),** в том числе: | 40 | 40 |
| подготовка к зачету | 36 | 36 |
| подготовка к практическим занятиям | 4 | 4 |
| **Итого: час** | 72 | 72 |

| | | |
|---|---|---|
| **Итого: з.е.** | 2 | 2 |

## 4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

| № раздела | Наименование раздела дисциплины | Виды учебной нагрузки и их трудоемкость, часы | | | | |
|---|---|---|---|---|---|---|
| | | ЛЗ | ЛР | ПЗ | СРС | Всего часов |
| 2 | Основы информационной безопасности | 16 | 0 | 16 | 40 | 72 |
| | **Итого** | 16 | 0 | 16 | 40 | 72 |

### 4.1 Содержание лекционных занятий

| № занятия | Наименование раздела | Тема лекции | Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов) | Количество часов / часов в электронной форме |
|---|---|---|---|---|
| **8 семестр** | | | | |
| 1 | Основы информационной безопасности | Введение в информационную безопасность. | Понятие информационной безопасности. Компьютерная безопасность. Доктрина ИБ РФ. Понятие угрозы, атаки, источника угроз, окна опасности. Классификация угроз. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности. | 2 |
| 2 | Основы информационной безопасности | Законодательный уровень информационной безопасности. | Законодательный уровень обеспечения ИБ. Конституция РФ. УК РФ в области защиты информации. Закон «О государственной тайне» и ответственность за его нарушение. Закон «О коммерческой тайне» и меры ответственности за его нарушение. Закон «О персональных данных». Закон «ОБ информации, информационных технологиях и о защите информации». Закон «О лицензировании отдельных видов деятельности». Основные лицензирующие органы и их функции. Нарушение авторских и смежных прав в Гражданском кодексе РФ. Кодекс об административных нарушениях РФ в области защиты информации. | 2 |

| | | | | |
|---|---|---|---|---|
| 3 | Основы информационной безопасности | Стандарты и спецификации в области информационной безопасности. | Техническая спецификация X.800. Сетевые средства безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Общие критерии»). Требования безопасности. Угрозы и уязвимые места. Профили защиты. «Общие критерии». Функциональный пакет. Функциональные требования. Требования доверия безопасности. | 2 |
| 4 | Основы информационной безопасности | Стандарты и спецификации в области информационной безопасности. | Сервисы безопасности. Гарантированность. Уровни гарантированности. Интерпретация «Оранжевой книги» для сетевых конфигураций. Сетевая доверенная вычислительная база. Руководящие документы Гостехкомиссии РФ. Классификация МЭ. Стандарт ИСО/МЭК 27001. ГОСТ Р ИСО/МЭК 17799-2005. | 2 |
| 5 | Основы информационной безопасности | Административный, процедурный и программно-технический уровень информационной безопасности. | Административный уровень ИБ. Понятие политики безопасности. Уровни политики безопасности (ПБ). Содержание ПБ верхнего уровня. Содержание ПБ среднего уровня. Содержание ПБ нижнего уровня. Процедурный уровень ИБ. Классы мер процедурного уровня и их содержание. Программно-технический уровень ИБ. Основные и вспомогательные сервисы безопасности. | 2 |
| 6 | Основы информационной безопасности | Сетевые атаки и сетевая защита. Экранирование и межсетевые экраны. Протоколы безопасности. | Прослушивание и сканирование сети. Генерация пакетов. Перехват данных. Имперсонация. Несанкционированный обмен данными. Принуждение к ускоренной передаче данных. Отказ в обслуживании. Классификация и типы атак. Системы обнаружения атак. Классификация. Средства анализа защищенности: сканирование, зондирование. Экранирование и межсетевые экраны. Основные понятия. Принципы работы межсетевых экранов. Классификация межсетевых экранов. Понятие демилитаризованной зоны. Пакетные фильтры. Сервера уровня соединения. Сервера прикладного уровня. Протокол SSL. Протокол SSH. Протокол S-HTTP. Протокол SOCKS. Протокол безопасности IPSec как набор стандартов для защиты данных и аутентификации на уровне IP. Туннельный и транспортный режим. VPN и протоколы туннелирования. | 2 |

| | | | | |
|---|---|---|---|---|
| 7 | Основы информационной безопасности | Вредоносное программное обеспечение и средства защиты от него. | Программные закладки: определения и классификация. Модели воздействия программных закладок на компьютеры. Способы воздействия на ЭЦП. Защита от программных закладок. Понятие изолированного компьютера. Троянские программы. Утилиты скрытого администрирования. Клавиатурные шпионы и их типы. Парольные взломщики. Понятие вируса. Классификация вирусов по различным признакам. Полиморфик-вирусы. Загрузочные вирусы. Макро-вирусы. Сетевые вирусы. Файловые вирусы. Антивирусное ПО. Классификация. | 2 |
| 8 | Основы информационной безопасности | Введение в криптографию. | Понятие криптографии. Основные определения. Классификация криптоалгоритмов по принципу действия. Симметричные и асимметричные алгоритмы. Классификация криптоалгоритмов по характеру воздействия на шифруемую информацию. Классификация по размеру обрабатываемых блоков: блочные и поточные алгоритмы. Сеть Фейстеля. Симметричные криптоалгоритмы, их параметры. Алгоритм ГОСТ 28147. Схема и режимы работы. Асимметричные алгоритмы. Основные требования, принципы действия, характеристики. Хэш-функции. Требования. Сильная хэш-функция. Назвать основные хэш-функции, принципы их действия, характеристики. Коды аутентификации сообщений MAC. Цифровая подпись. Требования к ЭЦП. Прямая и арбитражная цифровые подписи. Стандарт цифровой подписи DSS. Стандарт цифровой подписи ГОСТ 3410. | 2 |
| | | | **Итого за семестр:** | **16** |
| | | | **Итого:** | **16** |

## 4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

## 4.3 Содержание практических занятий

| **№ занятия** | **Наименование раздела** | **Тема практического занятия** | **Содержание практического занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов / часов в электронной форме** |
|---|---|---|---|---|
| **8 семестр** | | | | |
| 1 | Основы информационной безопасности | Введение. Основные понятия информационной безопасности | Введение. Основные понятия информационной безопасности | 2 |

| | | | | |
|---|---|---|---|---|
| 2 | Основы информационной безопасности | Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни | Воспитание ответственного отношения к информационной деятельности, связанной с обработкой и хранением информации; Приобретение опыта профилактической и предупреждающей деятельности по отношению к информационным угрозам на уровне личной информационной безопасности | 2 |
| 3 | Основы информационной безопасности | Применение методики управления рисками для анализа рисков личной информационной безопасности | Изучить методику для систематизации и анализа рисков по приведенным в приложении материалам курса С.А.Нестерова и "Руководства по управлению рисками". На основании собранных на лабораторном занятии №1 данных о неприкосновенность частной жизни идентифицировать риски личной информационной безопасности и создать их полное описание по определению методики. Выполнить этап "Поддержка принятия решений". Разработать план мероприятий по осуществлению этапов "Реализация контроля" и "Оценка эффективности программы". | 2 |
| 4 | Основы информационной безопасности | Анализ безопасности протокола обмена информацией | Найти уязвимость в схеме протокола. Определить, атака какого типа позволит воспользоваться выявленной уязвимостью протокола. Предложить способ модифицировать протокол, чтобы устранить уязвимость. | 2 |
| 5 | Основы информационной безопасности | Обзор функций безопасности Windows | Приобрести практические навыки использования технологий BitLocker, IPSec, MMC, UAC, встроенных в Windows. | 2 |
| 6 | Основы информационной безопасности | Разработка политики информационной безопасности | Разработать политику информационной безопасности подразделения с использованием общепринятых шаблонов и учетом специфики деятельности организации. | 2 |
| 7 | Основы информационной безопасности | Настройка Интернет-браузера для безопасной работы | Изучение настроек безопасности для различных браузеров. | 2 |
| 8 | Основы информационной безопасности | Аутентификация, разрешениями на файлы и папки Управление | Управления разрешениями на файлы и папки Windows. Управление доступом к файлам. | 2 |
| | | | **Итого за семестр:** | **16** |
| | | | **Итого:** | **16** |

## 4.4. Содержание самостоятельной работы

| **Наименование раздела** | **Вид самостоятельной работы** | **Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов** |
|---|---|---|---|

| 8 семестр | | | |
|---|---|---|---|
| Основы информационной безопасности | Подготовка к практическим занятиям | Изучение материала, содержащегося в указаниях для практических занятий. | 4 |
| Основы информационной безопасности | Подготовка к зачёту | Повторение материалов, содержащихся в лекционных и практических занятиях | 36 |
| | | **Итого за семестр:** | **40** |
| | | **Итого:** | **40** |

## 5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

| № п/п | Библиографическое описание | Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.) |
|---|---|---|
| Основная литература | | |
| 1 | Технологии и продукты Microsoft в обеспечении информационной безопасности; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu\|\|iprbooks\|\|102070 | Электронный ресурс |

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

## 6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

| № п/п | Наименование | Производитель | Способ распространения |
|---|---|---|---|
| 1 | Microsoft Windows | Microsoft (Зарубежный) | Лицензионное |

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

| № п/п | Наименование | Краткое описание | Режим доступа |
|---|---|---|---|
| 1 | Электронно-библиотечная система IPRbooks | http://www.iprbookshop.ru/ | Российские базы данных ограниченного доступа |

## 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

**Лекционные занятия**
401 (учебный корпус)

Компьютерный класс – учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – лингафонный кабинет.

Технические средства обучения, служащие для представления учебной информации большой аудитории, набор демонстрационного оборудования: экран, проектор, переносной ноутбук.

Оборудование: 18 компьютеров с выходом в сеть Интернет и с доступом в электронную информационно-образовательную среду СамГТУ.

Специализированная мебель: 18 компьютерных столов, 18 кресел-комфорт, стол и стул для преподавателя, доска.

**Практические занятия**
401 (учебный корпус)

Компьютерный класс – учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – лингафонный кабинет.

Технические средства обучения, служащие для представления учебной информации большой аудитории, набор демонстрационного оборудования: экран, проектор, переносной ноутбук.

Оборудование: 18 компьютеров с выходом в сеть Интернет и с доступом в электронную информационно-образовательную среду СамГТУ.

Специализированная мебель: 18 компьютерных столов, 18 кресел-комфорт, стол и стул для преподавателя, доска.

**Самостоятельная работа**
209 (учебный корпус)

Помещение для самостоятельной работы – учебная аудитория для курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций.

Аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет» и с доступом в электронную информационно- образовательную среду СамГТУ.

Оборудование: 10 компьютеров с выходом в сеть Интернет.

Специализированная мебель:10 компьютерных стола, 10 стульев.

## 9. Методические материалы

## Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

## Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их

адекватности или эффективности в рассмотренной ситуации.

## Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчетности по данной работе.

## Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

## 10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
ФТД.02 «Основы информационной безопасности»

**Фонд оценочных средств**
**по дисциплине**
**ФТД.02 «Основы информационной безопасности»**

| | |
|---|---|
| **Код и направление подготовки (специальность)** | 13.03.02 Электроэнергетика и электротехника |
| **Направленность (профиль)** | Электроэнергетика |
| **Квалификация** | Бакалавр |
| **Форма обучения** | Очная |
| **Год начала подготовки** | 2020 |
| **Институт / факультет** | Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске |
| **Выпускающая кафедра** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Кафедра-разработчик** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Объем дисциплины, ч. / з.е.** | 72 / 2 |
| **Форма контроля (промежуточная аттестация)** | Зачет |

**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы**

| Наименование категории (группы) компетенций | Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции) |
|---|---|---|---|
| Универсальные компетенции | | | |
| Безопасность жизнедеятельности | УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуация и военных конфликтов | УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций | Владеть инструментами и методами защиты информации; механизмами реакции на инциденты; навыком распознавания заражений и точечных атак, действий хакеров; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. |
| | | | Знать основные концепции кибербезопасности; типы угроз; основные тренды в области защиты информации; методы и способы защиты от существующих угроз и кибератак; содержание информационной войны, методы и средства ее ведения; современные подходы к построению систем защиты информации; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; |

| | | | |
|---|---|---|---|
| | | | Уметь идентифицировать существующие и потенциальные риски; оценивать качество защиты данных; корректно и оперативно реагировать на инциденты безопасности; выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; |

## Матрица соответствия оценочных средств запланированным результатам обучения

| Код индикатора достижения компетенции | Результаты обучения | Оценочные средства | Текущий контроль успеваемости | Промежуточная аттестация |
|---|---|---|---|---|
| **Основы информационной безопасности** | | | | |
| УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций | **Уметь** идентифицировать существующие и потенциальные риски; оценивать качество защиты данных; корректно и оперативно реагировать на инциденты безопасности; выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; | вопросы | Да | Да |
| | **Владеть** инструментами и методами защиты информации; механизмами реакции на инциденты; навыком распознавания заражений и точечных атак, действий хакеров; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем. | вопросы | Да | Да |
| | **Знать** основные концепции кибербезопасности; типы угроз; основные тренды в области защиты информации; методы и способы защиты от существующих угроз и кибератак; содержание информационной войны, методы и средства ее ведения; современные подходы к построению систем защиты информации; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; | вопросы | Да | Да |