МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО

Декан факультета

Информационных технологий

_____ / А.Ю. Филиппович /

«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем» (специалитет)

Образовательная программа (профиль)

«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника

Специалист по защите информации

Форма обучения

Очная

Год приема - 2020

Москва 2020 г.

1. Цели и задачи дисциплины

К **основным целям** освоения дисциплины «Основы информационная безопасность» следует отнести:

- раскрытие сущности и значения информационной безопасности и методов защиты информации в практических задачах и их место в системе национальной безопасности;
- формирование у студентов научного мировоззрения, понимания важности научно обоснованных методов для решения профессиональных задач в области безопасности информационных технологий.

К **основным задачам** освоения дисциплины «Основы информационной безопасности» следует отнести:

- овладение студентами понятийным аппаратом в области информационной безопасности и защиты информации; установление и раскрытие структуры угроз защищаемой информации;
- изучение базовых содержательных положений в области информационной безопасности и защиты информации; раскрытие современной доктрины информационной безопасности;
- раскрытие различных форм представления информации в проблемах обеспечения информационной безопасности.
- ознакомление с современными подходами к решению общей задачи – созданию комплексной(-ых) системы(-ем) защиты информации

2. Место дисциплины в структуре ОП

Дисциплина «Основы информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части цикла Б.1 образовательной программы специалитета (Б.1.5) и взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП: Организационное и правовое обеспечение информационной безопасности , Криптографические методы защиты информации, Программно-аппаратные средства обеспечения информационной безопасности.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенция	В результате освоения образовательной программы	Перечень планируемых результатов обучения по дисциплине

	обучающийся должен обладать	
ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**знать:** значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации; **уметь:** определять информационные ресурсы, подлежащие защите, и угрозы безопасности информации; **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства;

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. 144 академические часа (лекции - 36 часов, лабораторные занятия - 36 часов, самостоятельная работа – 72 часа, форма контроля - зачет) в 1 семестре.

Содержание разделов дисциплины

Структура и содержание дисциплины «Информационная безопасность» по срокам и видам работы отражены в приложении.

Первый семестр

Тема 1. ***Введение.*** Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности, основная и дополнительная литература.

Тема 2. ***Защита информации как объективная закономерность эволюции постиндустриального общества.*** Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Глобализация информационных отношений. Информационные технологии. Информационные ресурсы услуги. Объективная необходимость и общественная потребность в защите информации. Сущность защиты информации. Правовое регулирование вопросов защиты информации.

Тема 3. ***Информационная безопасность личности, общества и государства: социально-правовые аспекты.*** Право на информацию в системе гражданских прав личности. Возможные ограничения. Массовая информация и информация ограниченного доступа. Неприкосновенность частной жизни, персональные данные. Виды тайн. Коммерческая тайна. Государственная тайна. Документированная информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности РФ. Информационные войны, информационное оружие. Доктрина информационной безопасности РФ.

Тема 4. ***Угрозы информационной безопасности в компьютерных системах.*** Компьютерная система (КС) как объект защиты информации. Понятие угрозы информационной безопасности в КС. Классификация и общий анализ угроз информационной безопасности в КС.

Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности.

Тема 5. ***Общая характеристика средств и методов защиты информации.*** Эволюция концепции информационной безопасности в компьютерных системах. Реализация угроз информационной безопасности путём несанкционированного доступа. Модель поведения потенциального нарушителя Обобщённые модели систем защиты информации. Основные принципы обеспечения информационной безопасности в КС. Понятие комплексной системы защиты информации (КСЗИ).

Тема 6. ***Организационно-правовое обеспечение защиты информации.*** Общая характеристика организационного обеспечения защиты информации. Основные задачи службы безопасности предприятия. Организационные мероприятия, обеспечивающие защиту информации. Необходимость правового регулирования в области защиты информации. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности; международные и отечественные нормативные и руководящие документы.

Тема 7. ***Защита информации в компьютерных системах от случайных угроз.*** Повышение эксплуатационной надежности КС. Сбои и отказы. Общие сведения о кодах для обнаружения и исправления случайных ошибок. Дублирование информации и резервирование технических средств. Блокировка ошибочных операций. Минимизация ущерба от аварий и стихийных бедствий.

Тема 8. ***Охрана объектов КС и средства защиты информации от утечки по техническим каналам.*** Система охраны объектов КС. Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Противодействие наблюдению в оптическом диапазоне. Противодействие подслушиванию. Методы и средства защиты от побочных электромагнитных излучений и наводок.

Тема 9. ***Защита компьютерных систем от несанкционированного вмешательства.*** Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования и исследования. Защита от несанкционированного изменения структуры КС в процессе эксплуатации. Контроль целостности программ и данных в процессе эксплуатации. Регистрация и контроль действий пользователей.

Тема 10. ***Криптографические методы защиты информации.*** Основные понятия и этапы развития криптографии. Классификация криптографических средств. Основные методы шифрования. Шифрование методами замены и перестановки. Аналитические и аддитивные методы шифрования. Системы шифрования с открытым ключом.

Тема 11. ***Компьютерные вирусы и средства антивирусной защиты.*** Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Механизмы заражения компьютерными вирусами. Методы и средства защиты от компьютерных вирусов. Профилактика заражения вирусами компьютерных систем

Тема 12. ***Комплексная защита информации в компьютерных системах.*** Концепция создания КСЗИ в КС. Технология разработки КСЗИ. Функционирование комплексных систем защиты информации. Аудит в защищенных КС. Организационная структура КСЗИ.

5. Образовательные технологии

Методика преподавания дисциплины «Основы информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению практических и домашних работ;
- проведение интерактивных лекционных занятий.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 25 % аудиторных занятий. Занятия лекционного типа составляют 50 % от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- устный опрос;
- проверка домашних заданий;
- зачёт.

Образцы тестовых заданий, контрольных вопросов проведения текущего контроля и зачёта приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины (модуля) формируются следующая компетенция:

Код компетенция	**В результате освоения образовательной программы обучающийся должен обладать**

ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

В процессе реализации образовательной программы осваивается данная компетенция, в том числе её отдельные компоненты, которые формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ОПК—1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности общества и государства				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации.	Обучающийся демонстрирует неполное соответствие следующих знаний: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих знаний: значение информации в развитии современного общества; информационные ресурсы, подлежащие защите, угрозы безопасности информации, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: значение информации в развитии современного общества, информационные ресурсы, подлежащие защите, угрозы безопасности информации, свободно оперирует приобретенными знаниями.
уметь: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации;	Обучающийся не умеет или в недостаточной степени умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации.	Обучающийся демонстрирует неполное соответствие следующих умений: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду	Обучающийся демонстрирует частичное соответствие следующих умений: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. Умения освоены, но допускаются незначительные ошибки,	Обучающийся демонстрирует полное соответствие следующих умений: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. Свободно

		показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства;	Обучающийся не владеет или в недостаточной степени владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.	Обучающийся владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях	Обучающийся частично владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, свободно применяет полученные навыки в ситуациях повышенной сложности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: зачет

Промежуточная аттестация обучающихся в форме зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка **«зачтено»** или **«не зачтено»**.

Шкала оценивания	Описание
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков, приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков, приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Федоров Н.В. Основы информационной безопасности. Электронный образовательный ресурс. Московский Политех, 2020- https://lms.mospolytech.ru/course/view.php?id=561

б) дополнительная литература:

1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350.

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. —

(Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

5. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285

6. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368

7. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083

8. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933

9. Криптографические методы и средства защиты информации. Бутакова Н.Г., Федоров Н.В. - Санкт-Петербург: ИЦ "Интермедия", 2019

10. Рагозин Ю. Н. Инженерно-техническая защита информации: учебное пособие - Санкт-Петербург: ИЦ "Интермедия", 2018

11. Семененко В.А. Информационная безопасность : учеб. пособие для вузов. - 3-е издание Гриф УМО, 2012

12. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов. - М.: Горячая линия-Телеком, Гриф МО.

13. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432с.

14. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методические основы. МГИУ, 2009 - 367с.

в) программное обеспечение и Интернет-ресурсы:

1. http://bibliotekar.ru/biznes-29/index.htm
2. http://citforum.ru/security/
3. http://www.itsec.ru/main.php
4. http://www.securrity.ru/
5. Локальный электронный учебник по направлению «Информационная безопасность» для бакалавров и специалистов. Федоров Н.В. Свидетельство о государственной регистрации программы для ЭВМ № 2013610300.
6. Операционная система Windows 7(или ниже) – Microsoft Open License.

Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215.

7. Офисные приложения, Microsoft Office 2013(или ниже) – Microsoft Open License. Лицензия № 61984042.

8. Материально-техническое обеспечение дисциплины

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, компьютер, экран) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачёту, а также самостоятельно изучают отдельные темы учебной программы.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на зачете в письменной и устной форме.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов **10.05.03 «Информационная безопасность автоматизированных систем».**

Программу составил: проф. Федоров Н.В.

Программа утверждена на заседании кафедры «Информационная безопасность»

«28» мая 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

проф. к.т.н., Н.В. Федоров

Структура и содержание дисциплины
«Основы информационной безопасности»
Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалитет)
Форма обучения: Очная

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб.	СРС	КСР	К.Р.	К.П.	РГР	Реферат	К/р	Э	З
	Первый семестр														
1	**Тема 1.** Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности.	1	0,5	1		-	2								
2	**Тема 2.** Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе.	1	2.5	3		2	6								
3	**Тема 3.** Информационная безопасность личности, общества и государства: социально-правовые аспекты	1	3,5-5	2		2	6								
4	**Тема 4.** Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в компьютерных системах**.**	1	6	3		4	8								
5	**Тема 5** Эволюция концепции информационной безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации.	1	7-8	2		4	8								
6	**Тема 6.** Общая характеристика организационного обеспечения защиты информации. Организационно-правовое обеспечение защиты информации.	1	9	2		2	6								
7	**Тема 7.** Повышение эксплуатационной надежности КС. Защита информации в компьютерных системах от случайных угроз.	1	10	3		2	6								
8	**Тема 8.** . Охрана объектов КС и средства защиты информации от утечки по техническим каналам. Противодействие подслушиванию. Методы и средства защиты КС от побочных электромагнитных излучений и наводок.	1	11- 12	4		4	8								

9	**Тема 9.** Защита КС от несанкционированного вмешательства. Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам	1	13-14	4		4	4								
10	**Тема 10** Криптографические методы защиты информации. Основные понятия и методы шифрования**.**	1	15	4		4	6								
11	**Тема** 11 Компьютерные вирусы и средства антивирусной защиты. Общие сведения о компьютерных вирусах Профилактика заражения вирусами компьютерных систем	1	16	4		4	6								
12	**Тема 12** Комплексная защита информации в компьютерных системах (КСЗИ). Концепция создания КСЗИ в КС. Функционирование КСЗИ.	1	17-18	4		4	6								
	Форма аттестации														**З**
	Всего часов по дисциплине в первом семестре		144	36		36	72								
	Всего часов по дисциплине		144	36		36	72								

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «**Информационная безопасность автоматизированных систем»**
ОП (профиль): **«Обеспечение информационной безопасности распределённых информационных систем»**
Форма обучения: **очная**

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Основы информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

1. Описание оценочных средств:

Составитель:
проф. Федоров Н.В.

Москва, 2020 год

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Обеспечение информационной безопасности распределённых информационных систем					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общие компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средств**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ОПК—1	способен оценивать роль ин формации, информационны технологий и информацион ой безопасности в совре енном обществе, их зна ение для обеспечения объек ивных потребностей личности общества и государства	**знать:** значение информации в развитии современного общества; информационные ресурсы, подлежащи защите, угрозы безопасности информации; **уметь:** определять информационные ресурсы, подлежа щие защите, и угрозы безопасности информации; **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства;	лекции, самостоятельная работа, лабораторные занятия	коллоквиум зачет	**Базовый уровень** -знать значение информации в развитии современного общества; информационные ресурсы, подлежащие -защите, угрозы безопасности информации -уметь определять информационные ресурсы, подлежащие защите, угрозы безопасности информации. - владеть **Повышенный уровень** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

Оценочные средства для текущей аттестации

Электронный тест

Оценочные средства для промежуточной аттестации

Зачет.

Список вопросов для зачета по дисциплине.

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
3. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
4. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
5. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
6. Общая характеристика случайных угроз информационной безопасности в КС.
7. Общая характеристика преднамеренных угроз информационной безопасности в КС.
8. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
9. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.
10. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
11. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
12. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, и правообладателя информационных ресурсов.
13. Отечественное законодательство в области информации и защиты информации.
14. Ответственность за правонарушения при работе с компьютерными системами.

15. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.
16. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.
17. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.
18. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование. Технология RAID.
19. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.
20. Система охраны объектов КС.
21. Общая характеристика технических каналов утечки информации в КС.
22. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.
23. Средства противодействия подслушивания и дистанционному наблюдению.
24. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
25. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.
26. Средства и методы разграничения доступа к ресурсам КС.
27. Защита программных средств КС от несанкционированного копирования и исследования.
28. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.
29. Контроль целостности программ и данных в процессе эксплуатации КС.
30. Общие понятия, история развития и классификация криптографических средств.
31. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
32. Шифрование методом замены. Простая, полиалфавитная и многозначная замена.
33. Шифрование методом перестановки. Маршрутные перестановки. Поворотные решетки.
34. Аналитические методы шифрования.
35. Шифрование методом гаммирования.
36. Системы шифрования с открытым ключом. Односторонние функции. Электронная цифровая подпись. Алгоритм шифрования RSA.
37. Отечественные и зарубежные стандарты шифрования.
38. Общая характеристика и классификация компьютерных вирусов.
39. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
40. Средства, используемые для обнаружения компьютерных вирусов.
41. Профилактика заражения компьютерными вирусами.
42. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.
43. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.

44. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
45. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.
46. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.
47. Основные технологические этапы разработки КСЗИ.
48. Средства моделирования, применяемые для оптимизации КСЗИ.
49. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.
50. Задачи, решаемые подсистемой аудита в составе защищенных КС.