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

«Программно-аппаратные средства защиты информации»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Программно-аппаратные средства защиты информации» следует отнести:

- ознакомление студентов с современными программно-аппаратными средствами защиты информации в компьютерных системах;
- овладение методами решения задач программно-аппаратной защиты информации.

К **основным задачам** освоения дисциплины «Программно-аппаратные средства защиты информации» следует отнести:

- обучение студентов современным методам программно-аппаратной защиты информации;
- приобретение профессиональной компетентности в программно-аппаратных средствах защиты информации;
- умение ориентироваться в продуктах и тенденциях развития средств программно-аппаратной защиты информационных технологий.

2. Место дисциплины в структуре ООП бакалавриата.

Дисциплина «Программно-аппаратные средства защиты информации » относится к числу профессиональных учебных дисциплин вариативной части цикла (Б.1.ДВ - дисциплины по выбору студента) основной образовательной программы бакалавриата (Б.1.ДВ.8).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты информации».

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

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

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК - 1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	**знать:** - возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; механизмы решения типовых задач программно-аппаратной защиты информации; **уметь:** -анализировать механизмы реализации программно-аппаратных методов защиты конкретных объектов и процессов для решения профессиональных задач; -применять штатные средства программно-аппаратной защиты и специализированные продукты для решения типовых задач; -квалифицированно оценивать область применения

		конкретных механизмов программно-аппаратной защиты информации; -использовать аппаратные и программные средства защиты информации при решении практических задач. - организовать его внедрение и последующее сопровождение; - выполнять работы по установке, настройке и обслуживанию программно-аппаратных средств защиты информации. **владеть:** - навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.
ПК - 3	способностью администрировать подсистемы информационной безопасности объекта защиты;	**уметь:** - администрировать подсистемы информационной безопасности объекта защиты; **владеть:** - навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, курсовой проект, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Программно-аппаратные средства защиты информации» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема1. Понятие политики безопасности при программно-аппаратной защите информации.

Разработка политики информационной безопасности. Методология политики безопасности компьютерных систем. Основные положения политики информационной безопасности. Жизненный цикл политики безопасности. Принципы политики безопасности.

Тема 2. Архитектура системы программно-аппаратной защиты.

Объекты угроз. Классификация угроз по способу их осуществления. Классификация объектов угроз. Функциональная модель системы защиты. Состав и назначение функциональных блоков. Основные группы механизмов защиты. Функциональная модель. Рекомендации по отдельным уровням функциональной модели.

Тема 3. Модель компьютерной системы.

Понятие доступа и монитора безопасности. Обеспечение гарантий выполнения политики безопасности. Методология проектирования гарантированно защищенных КС. Метод генерации изолированной программной среды.

Тема 4. Модели типовых политик безопасности компьютерных средств защиты информации.

Дискреционные модели. Модель АДЕПТ-50. Пятимерное пространство безопасности Хартстона. Мандатная модель. Модель Белла-Лападула. Первое правило модели Белла-Лападула. Второе правило модели Белла-Лападула. Описание модели.

Тема 5. Программно-аппаратные средства идентификации и аутентификации пользователей.

Идентификация и аутентификация. Основные понятия и классификация. Простая аутентификация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе сертификатов. Биометрическая идентификация и аутентификация пользователей.

Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций. Аутентификация с использованием асимметричных алгоритмов шифрования. Аутентификация, основанная на использовании цифровой подписи. Протоколы аутентификации с нулевой передачей значений. Упрощенная схема аутентификации с нулевой передачей знаний. Параллельная схема аутентификации с нулевой передачей знаний. Инфраструктура открытых ключей.

Тема 6. Механизм идентификации и аутентификации в ОС. Разграничение доступа.

Протокол идентификации и аутентификации в ОС Windows. Протокол аутентификации Kerberos. Сохранность паролей учетных записей. Windows. Защита паролей. Кража SAM-файла. Захват привилегий. Сброс пароля. Взлом вторичных паролей. Система разграничения доступа ОС LINUX. Возможности стандартной системы разграничения доступа ОС Linux. Недостатки стандартной системы разграничения доступа ОС Linux. Возможности наиболее известных средств совершенствования разграничения доступа ОС Linux.

Тема 7. Защита файловой системы в ОС.

Защита файловой системы Windows. Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System. Технология шифрования. Восстановление данных. Процесс шифрования. Процесс дешифрирования. Процесс восстановления. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Типовые задачи администрирования. Администрирование дисков в Windows. Сходства и различия между Disk Management и Disk Administrator. Защита файловой системы OS Linux. Файловая система OS Linux. Основные концепции файловой системы. Виртуальная Файловая Система (VFS). Файловые системы EXT2 (The Second Extended File System).

5. Образовательные технологии.

Методика преподавания дисциплины «Программно-аппаратные средства защиты информации» 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 лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % 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:

- компьютерное тестирование;
- экзамен.

Образцы тестовых заданий, экзаменационных билетов, 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 следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК - 1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК - 3	способностью администрировать подсистемы информационной безопасности объекта защиты

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, 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 (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК - 1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

знать: - возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; механизмы решения типовых задач программно-аппаратной защиты информации;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; механизмы решения типовых задач программно-аппаратной защиты информации.	Обучающийся демонстрирует неполное соответствие следующих знаний: возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; механизмы решения типовых задач программно-аппаратной защиты 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: возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; механизмы решения типовых задач программно-аппаратной защиты информации , но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; механизмы решения типовых задач программно-аппаратной защиты информации , свободно оперирует приобретенными знаниями.
уметь: анализировать механизмы реализации программно-аппаратных методов защиты конкретных объектов и процессов для решения профессиональных задач; -применять штатные средства программно-аппаратной защиты и специализированные продукты для решения типовых задач; -квалифицированно оценивать область применения конкретных механизмов программно-аппаратной защиты информации; -использовать	Обучающийся не умеет или в недостаточной степени умеет анализировать механизмы реализации программно-аппаратных методов защиты конкретных объектов и процессов для решения профессиональных задач; -применять штатные средства программно-аппаратной защиты и специализированные продукты для решения типовых задач; выполнять работы по установке, настройке и обслуживанию	Обучающийся демонстрирует неполное соответствие следующих умений: анализировать механизмы реализации программно-аппаратных методов защиты конкретных объектов и процессов для решения профессиональных задач; -применять штатные средства программно-аппаратной защиты и специализированные продукты для решения типовых задач . выполнять работы по установке, настройке и обслуживанию программно-аппаратных средств защиты информации . Допускаются значительные ошибки, проявляется	Обучающийся демонстрирует частичное соответствие следующих умений: выполнять работы по установке, настройке и обслуживанию программно-аппаратных средств защиты информации . Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: выполнять работы квалифицированно оценивать область применения конкретных механизмов программно-аппаратной защиты информации; -использовать аппаратные и программные средства защиты информации при решении практических задач. - организовать его внедрение и последующее сопровождение; по установке, настройке и обслуживанию программно-

аппаратные и программные средства защиты информации при решении практических задач. - организовать его внедрение и последующее сопровождение; - выполнять работы по установке, настройке и обслуживанию программно-аппаратных средств защиты информации;	программно-аппаратных средств защиты информации.	недостаточность умений.		аппаратных средств защиты информации . Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: - навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.	Обучающийся не владеет или в недостаточной степени владеет навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита).	Обучающийся владеет, допускаются значительные ошибки, навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита), проявляется недостаточность владения навыками.	Обучающийся частично владеет навыками квалифицированно оценивать область применения конкретных механизмов программно-аппаратной защиты информации; -использовать аппаратные и программные средства защиты информации при решении практических задач; эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита), навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита), свободно применяет полученные навыки в ситуациях повышенной сложности.
ПК - 3 способностью администрировать подсистемы информационной безопасности объекта защиты				
уметь: - администрировать подсистемы информационной безопасности объекта защиты;	Обучающийся не умеет или в недостаточной степени умеет администрировать подсистемы информационной безопасности	Обучающийся демонстрирует неполное соответствие следующих умений: администрировать подсистемы информационной безопасности объекта	Обучающийся демонстрирует частичное соответствие следующих умений: администрировать подсистемы информационной	Обучающийся демонстрирует полное соответствие следующих умений: администрировать подсистемы информационной безопасности

	объекта защиты.	защиты . Допускаются значительные ошибки, проявляется недостаточность умений.	безопасности объекта защиты . Умения освоены, но допускаются незначительные ошибки, неточности.	объекта защиты . Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: - навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.	Обучающийся не владеет или в недостаточной степени владеет навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита).	Обучающийся владеет навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита), допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) , навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита), свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена 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 по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	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.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.

Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	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. . Программно-аппаратные средства защиты информации. Электронный образовательный ресурс. Московский Политех, 2020- https://lms.mospolytech.ru/course/view.php?id=495

б) дополнительная литература:

1. А.Ю.Щербаков Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачева С.В., 2001 - 352с.
2. А.А. Грушо, Е.Е. Тимонина Теоретические основы защиты информации. М.: Яхтсмен, 1996 - 192с.
3. Семененко В.А. Программно-аппаратная защита информации :учеб. пособие. / Федоров Н.В. - М.: МГИУ, 2007 Гриф УМО
4. Программно-аппаратная защита информации :метод. указ. по курс. проектированию 28-8. / сост. Федоров Н.В. - М.: МГИУ, 2008
5. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для вузов. - М.: Академия, 2005 Гриф УМО

в) программное обеспечение и интернет-ресурсы:

1. Локальный научно-образовательный комплекс по дисциплине "Программно-аппаратная защита информации".

8. Материально-техническое обеспечение дисциплины.

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

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

Оборудование и аппаратура.

1. Электронный замок "Соболь".
2. Система защиты "Secret Net".
3. ПАК защищенного хранения информации «Секрет Особого Назначения»

4. Комплекс средств защиты информации от НСД «Аккорд–АМДЗ»
5. ПАК защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 5.0).

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, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

Программу составил: проф., к.т.н. Федоров Н.В.

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Программно-аппаратные средства защиты информации»
по направлению подготовки
10.03.01 «Информационная безопасность»
(бакалавр)

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.	ДЗ	Реферат	К/р	Э	З
	Седьмой семестр														
1	Самостоятельная работа														
1.1	Разработка политики информационной безопасности. Методология политики безопасности компьютерных систем. Основные положения политики информационной безопасности. Жизненный цикл политики безопасности. Принципы политики безопасности.	7	1				4								
1.2	Разработка политики информационной безопасности компьютерной системы.	7	2				4								
1.3.	Разработка модели угроз компьютерной системы.	7	3				4								
1.4	Объекты угроз. Классификация угроз	7	4				4								

	по способу их осуществления. Классификация объектов угроз. Функциональная модель системы защиты. Состав и назначение функциональных блоков. Основные группы механизмов защиты. Функциональная модель. Рекомендации по отдельным уровням функциональной модели.														
1.5	Дискреционные и мандатные модели.	7	5				4								
1.6	Система защиты информации от несанкционированного доступа «СТРАЖ NT». Установка и снятие СЗИ. Замкнутая программная среда.	7	6				4								
1.7	Система защиты информации от несанкционированного доступа «СТРАЖ NT». Управление пользователями. Учет носителей и контроль устройств.	7	7				4								
1.8	Понятие доступа и монитора безопасности. Обеспечение гарантий выполнения политики безопасности. Методология проектирования гарантированно защищенных КС. Метод генерации изолированной программной среды.	7	8				4								
1.9	Дискреционные модели. Модель АДЕПТ-50. Пятимерное пространство безопасности Хартстона. Мандатная модель. Модель Белла-Лападула. Первое	7	9				4								

	правило модели Белла-Лападула. Второе правило модели Белла-Лападула. Описание модели.														
1.10	Идентификация и аутентификация. Основные понятия и классификация. Простая аутентификация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе сертификатов. Биометрическая идентификация и аутентификация пользователей.	7	10				4								
1.11	Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций. Аутентификация с использованием асимметричных алгоритмов шифрования. Аутентификация, основанная на использовании цифровой подписи. Протоколы аутентификации с нулевой передачей значений. Упрощенная схема аутентификации с нулевой передачей знаний. Параллельная схема аутентификации с нулевой передачей знаний.	7	11				4								
1.12	Протокол идентификации и	7	12				4								

	аутентификации в ОС Windows.														
1.13	Протокол идентификации и аутентификации в ОС Windows. Протокол аутентификации Kerberos. Сохранность паролей учетных записей. Windows. Защита паролей. Кража SAM-файла. Захват привилегий. Сброс пароля. Взлом вторичных паролей. Система разграничения доступа ОС LINUX. Возможности стандартной системы разграничения доступа ОС Linux. Недостатки стандартной системы разграничения доступа ОС Linux. Возможности наиболее известных средств совершенствования разграничения доступа ОС Linux.	7	13				4								
1.14	Протокол аутентификации Kerberos.	7	14				4								
1.15	Система разграничения доступа ОС LINUX.	7	15				4								
1.16	Защита файловой системы Windows. Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System. Технология шифрования. Восстановление данных. Процесс шифрования. Процесс дешифрирования. Процесс восстановления. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Типовые задачи	7 7	16				4								

	администрирования. Администрирование дисков в Windows. Сходства и различия между Disk Management и Disk Administrator.														
1.17	Шифрующая файловая система (EFS) Encrypting File System.	7	17				4								
1.18	Защита файловой системы OS Linux. Файловая система OS Linux. Основные концепции файловой системы. Виртуальная Файловая Система (VFS). Файловые системы EXT2 (The Second Extended File System).	7	18				4								
2	Лабораторные работы														
2.1	Установка и инициализация комплекса «Соболь». Настройка общих параметров	7	1			4									
2.2	Настройка и эксплуатация комплекса «Соболь»	7	2			4									
2.3	Установка и инициализация комплекса «Secret Net 5.0-C». Настройка общих параметров	7	3			4									
2.4	Управление режимами входа в систему. Управление персональными идентификаторами пользователей.	7	4			4									
2.5	Управление устройствами в Secret Net 5.0.	7	5			4									
2.6	Полномочное разграничение доступа в Secret Net 5.0.	7	6			4									
2.7	Контроль целостности и замкнутая	7	7-8			8									

	программная среда в Secret Net 5.0														
2.8	Шифрование файлов в Secret Net 5.0.	7	9			4									
2.9	Администрирование ПАК защищенного хранения информации «Секрет Особого Назначения»	7	10			4									
2.10	Использование ПАК защищенного хранения информации «Секрет Особого Назначения» авторизованным пользователем	7	11			4									
2.11	Установка и инициализация комплекса средств защиты информации от НСД «Аккорд–АМДЗ»	7	12			4									
2.12	Администрирование комплекса средств защиты информации от НСД «Аккорд–АМДЗ»	7	13			4									
2.13	Установка и инициализация ПАК защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 5.0)	7	14			4									
2.14	Установка правил разграничения доступа. Программа ACED32. Дискреционный метод ПРД.	7	15			4									
2.15	Установка правил разграничения доступа. Программа ACED32. Мандатный метод контроля ПРД	7	16			4									
2.16	Установка правил разграничения доступа. Программа ACED32. Стартовая задача пользователя.	7	17			4									
2.17	Установка правил разграничения доступа. Программа ACED32.	7	18			4									

	Контроль целостности файлов														
	Форма аттестации	7	19-21							.				Э	
	Всего часов по дисциплине во седьмом семестре					72	72								
	Всего часов по дисциплине					72	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗРВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем систем

(кибербезопасность новой информационной среды)»

Форма обучения: очная

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

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Программно-аппаратные средства защиты информации»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Компьютерное тестирование

Экзамен

Составители: к.т.н., доцент Федоров Н.В.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Программно-аппаратные средства защиты информации					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК - 1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	**знать:** - возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; - механизмы решения типовых задач программно-аппаратной защиты информации; **уметь:** -анализировать механизмы реализации программно-аппаратных методов защиты конкретных объектов и процессов для решения профессиональных задач; -применять штатные средства программно-аппаратной защиты и специализированные продукты для решения типовых задач; -квалифицированно оценивать область применения конкретных механизмов программно-аппаратной защиты информации; -использовать аппаратные и программные средства защиты информации при решении практических задач. - организовать его внедрение и последующее сопровождение; - выполнять работы по установке, настройке и обслуживанию программно-аппаратных средств защиты информации; **владеть:** - навыками эксплуатации (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.	самостоятельная работа, лабораторные занятия	КТ, экзамен	Базовый уровень: знать: - возможные действия противника, направленные на нарушение политики безопасности информации; - наиболее уязвимые для атак противника элементы компьютерных систем; - механизмы решения типовых задач программно-аппаратной защиты информации; умеет выполнять работы по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) средств защиты информации; Повышенный уровень: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) средств защиты информации;

ПК - 3	способностью администрировать подсистемы информационной безопасности объекта защиты;	**уметь:** - администрировать подсистемы информационной безопасности объекта защиты; **владеть:** - навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.	самостоятельная работа, лабораторные занятия	КТ, экзамен	Базовый уровень: умеет администрировать подсистемы информационной безопасности объекта защиты; Повышенный уровень: владеет навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Компьютерное тестирование.

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1. Компьютерная система как объект защиты информации
2. Понятие угрозы информационной безопасности в КС
3. Классификация и общий анализ угроз информационной безопасности в КС
4. Случайные угрозы информационной безопасности КС
5. Преднамеренные угрозы информационной безопасности КС
6. Разработка политики информационной безопасности КС
7. Методология политики безопасности компьютерных систем
8. Основные положения политики информационной безопасности КС
9. Жизненный цикл политики безопасности КС
10. Функциональная модель системы защиты. Состав и назначение функциональных блоков
11. Понятие доступа и монитора безопасности
12. Методология проектирования гарантированно защищенных КС
13. Метод генерации изолированной программной среды
14. Модель АДЕПТ-50
15. Пятимерное пространство безопасности Хартстона
16. Мандатная модель доступа
17. Модель Белла-Лападула
18. Идентификация и аутентификация. Основные понятия и классификация
19. Простая аутентификация
20. Электронный замок "Соболь"
21. Биометрическая идентификация и аутентификация пользователей
22. Строгая аутентификация
23. Протоколы аутентификации с симметричными алгоритмами шифрования
24. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций
25. Аутентификация с использованием асимметричных алгоритмов шифрования
26. Аутентификация, основанная на использовании цифровой подписи
27. Протоколы аутентификации с нулевой передачей значений
28. Упрощенная схема аутентификации с нулевой передачей знаний
29. Параллельная схема аутентификации с нулевой передачей знаний
30. Протокол аутентификации Kerberos
31. Протокол идентификации и аутентификации в ОС Windows

32. Сохранность паролей учетных записей
33. Защита информации в файловой системе NTFS
34. Шифрующая файловая система (EFS) Encrypting File System
35. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing)
36. Администрирование дисков в Windows
37. Windows: Защита паролей
38. Возможности стандартной системы разграничения доступа ОС Linux
39. Система LIDS
40. Формат сертификатов открытых ключей X.509
41. Инфраструктура открытых ключей
42. Теоретические принципы построения биометрических систем
43. Вектор параметров при анализе рукописного почерка
44. Защита на уровне расширений BIOS
45. Защита на уровне загрузчиков операционной системы
46. Сертификат открытых ключей X.509

Пример билета.

1. Компьютерное тестирование.

2. Аутентификация с использованием асимметричных алгоритмов шифрования.

3. Практическая настройка программно-аппаратных средств защиты.