Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
ОТДЕЛЕНИЕ ПРИКЛАДНОЙ ИНФОРМАТИКИ

кафедра Системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры Системного анализа и информатики

Протокол №6 от «2» сентября 2019г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.07.01 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

направление подготовки
09.03.03 «Прикладная информатика»
направленность (профиль)
«Прикладная информатика в информационной безопасности»
квалификация
бакалавр
очная форма обучения

Год набора – 2020

Москва, 2020 г.

Автор–составитель: к.т.н.
доцент кафедры Системного анализа и информатики Каширская Е.Н.

Заведующий кафедрой
Системного анализа и информатики Маруев С.А

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Программно-аппаратные средства защиты информации» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-6	способен собирать детальную информацию для формализации требований пользователей заказчика	ПК-6.3	Способен документировать полученные данные на основании регламентов организации
ПК-7	способен проводить описание прикладных процессов и информационного обеспечения решения прикладных задач	ПК-7.1	Способен выбирать методы и средства описания прикладных процессов в решении прикладных задач
ПК-18	способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-18.2	ПК-18.2 Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Код этапа освоения компетенции	Результаты обучения
ПК-6.3	на уровне знаний: знать методы анализа предметной области информационных потребностей и формирования требований к информационной системе;
	на уровне умений: уметь проводить анализ предметной области, выявлять информационные потребности пользователей заказчика;
	на уровне навыков: обладать навыками применения методов и инструментальных средств описания и анализа требований пользователей заказчика.
ПК-7.1	на уровне знаний: знать теорию и средства проектирования структур данных, информационных процессов и информационного обеспечения решения прикладных задач;
	на уровне умений: уметь анализировать и описывать информационные процессы и информационное обеспечение решения прикладных задач;
	на уровне навыков: иметь навыки применения современных инструментальных средств при описании и проектировании информационных процессов и информационного обеспечения решения прикладных задач.

ПК-18.2	на уровне знаний: знать виды угроз безопасности, методы и средства обеспечения информационной безопасности, подходы к организации ИТ - инфраструктуры;
	на уровне умений: уметь организовывать защиту информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);
	на уровне навыков: иметь навык обеспечения информационной безопасности и защиты информации, организации ИТ – инфраструктуры.

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах – 3 ЗЕ (108/81 ч).
Количество академических/астрономических часов, выделенных на контактную работу по очной форме обучения – 64/48 часов (в т.ч. лекц. - 32 ч., практ.-32 ч.); на самостоятельную работу обучающихся на очной форме – 44/33 часа.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.07.01 «Программно-аппаратные средства защиты информации» относится к дисциплинам по выбору вариативной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.
Дисциплина изучается на 2 курсе в 4 семестре (очная форма обучения)
Дисциплина опирается на объём знаний, полученных при изучении таких дисциплин, как Информатика, Программирование и алгоритмизация, Операционные системы, Информационные системы и технологии, Теоретические основы компьютерной безопасности, Основы информационной безопасности.
Форма промежуточной аттестации – зачет.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Защита программ и данных	20	6		6		8	Д, О
Тема 2	Защита в операционных системах	22	6		6		10	Д, О
Тема 3	Защита в сетях	26	8		8		10	Д, О
Тема 4	Защита в СУБД	26	8		8		10	Д, О

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 5	Нормативно-правовые основы применения, сертификации средств и систем защиты информации	14	4		4		6	Д, О
Промежуточная аттестация		зачет						
Всего академ./астроном.часов:		**108/81**	**32/24**		**32/24**		**44/33**	

Примечание: * – формы текущего контроля успеваемости: доклад(ы) (Д), опрос (О).

Содержание дисциплины

№ п/п	Название темы	Основные вопросы и положения, раскрывающие содержание темы
Тема 1	**Защита программ и данных.**	Защищаемая информация и основные способы несанкционированного доступа (НСД) в автоматизированной системе: виды информации, подлежащей защите; классификация угроз безопасности; модель нарушителя; основные методы и средства защиты информации. Роль и место программно-аппаратных средств информационной безопасности в КСЗИ: классификация средств защиты информации (СЗИ); основные функции средств защиты информации от НСД. Механизмы защиты, реализуемые в программно-аппаратных СЗИ от НСД: управление доступом; регистрация и контроль критичных событий; контроль целостности данных; криптографическая защита; примеры средств защиты информации от НСД. Защита от разрушающих программных воздействий: понятие РПВ; взаимодействие прикладной программы и программной закладки; методы внедрения закладок; компьютерные вирусы как особый класс РПВ; защита от РПВ; антивирусные

		программы. Резервирование и восстановление данных: методы и схемы резервного копирования; запоминающие устройства для хранения резервных копий; план резервного копирования; примеры средств резервного копирования. Защита программного обеспечения от изучения и копирования: проблемы защиты ПО от несанкционированного изучения и использования; программно-аппаратные методы защиты ПО от несанкционированного использования; организационно-правовые методы защиты ПО от несанкционированного использования; защита ПО от изучения; способы и программы, позволяющие обходить методы защитыПО.
Тема 2	**Защита в операционных системах**	Общие сведения об операционных системах: назначение и функции операционной системы, особенности архитектуры операционных систем; классификация операционных систем, тенденции развития операционных систем; файловые системы. Угрозы безопасности и типичные атаки на операционную систему: классификация угроз безопасности, типичные атаки на операционную систему; особенности операционной системы, негативно влияющие на ее защищенность. Типовая структура подсистемы безопасности ОС и выполняемые ей функции: принципы проектирования защищенных систем; подходы к созданию защищенных ОС; основные функции подсистемы безопасности ОС; идентификация,аутентификация, авторизация; разграничение доступа в ОС; домен безопасности;аудит. Средства обеспечения безопасности в ОС семейства Windows. Основы безопасности в ОС семейства UNIX.
Тема 3	**Защита в сетях**	Введение в сетевую безопасность: преимущества использования сети Интернет и каналы утечки, связанные с ним; базовые принципы сетевого взаимодействия; модель взаимодействия открытых систем OSI; стек протоколов TCP/IP; механизмы реализации сетевых атак; обзор механизмов защиты компьютерных сетей. Межсетевые экраны: понятие периметра сети; определение и функции межсетевого экранирования; фильтрация трафика; трансляция адресов; классификация межсетевых экранов; инспекторы состояния; примеры межсетевых экранов. Основы криптографических методов защиты информации: задачи, достоинства и недостатки криптографических методов защиты информации; классификация криптографических методов защиты информации; хеширование; симметричные алгоритмы; асимметричные алгоритмы; аутентификация данных и электронная подпись; требования к криптографическим системам защиты. Технология VPN: определение и разновидности VPN-

		технологий;специфика построения VPN-сети; требования к VPN-технологиям; реализация VPN-технологий, примеры. Сканеры безопасности: классификация уязвимостей; каталоги уязвимостей; применение сканеров безопасности; классификация сканеров безопасности; примеры сканеров безопасности. Системы обнаружения вторжений (СОВ): определение систем обнаружения вторжений и цели их использования; классификация СОВ; архитектура СОВ; схема работы СОВ; методы обнаружения вторжений; системы предотвращения вторжений; стандарты в области СОВ.
Тема 4	**Защита в СУБД.**	Введение в безопасность СУБД: объекты защиты, уязвимости СУБД, особенности защиты информации в базах данных, критерии защищенности СУБД; Средства обеспечения безопасности данных в базе: идентификация и аутентификация пользователей, управление доступом, регистрация событий безопасности, представления, триггеры, особенности шифрования данных, транзакции. Обеспечение целостности базы данных: ограничения и ссылочная целостность, правила, использование хранимых процедур и триггеров, резервное копирование и восстановление, контрольные точки. Обеспечение безопасности данных в распределенных базах данных: кластерная организация сервера баз данных, защита коммуникаций между сервером и клиентами, проблемы параллелизма, сериализация транзакций, блокировки, тиражирование данных и синхронизация. Примеры реализации системы защиты в СУБД: Microsoft Access, MS SQLServer.
Тема 5	**Нормативно-правовые основы применения, сертификации средств и систем защиты информации.**	Общие сведения о стандартизации в области защиты информации. Понятиестандартизации. Роль стандартов в области защиты информации. Оценочные стандарты и технические спецификации. Преимущества и недостатки стандартизации. Стандарты и регулирование. Международные и зарубежные стандарты в области защиты информации. Критерии безопасности компьютерных систем Министерства обороны США «Оранжевая книга». Европейские критерии безопасности информационных технологий. Американские Федеральные критерии безопасности информационных технологий. Общие критерии безопасности информационных технологий. Рекомендации X.800. Британский стандарт BS 7799. Семейство международных стандартов на системы управления информационной безопасностью 27000. Стандарты ISO/IEC 27002– ГОСТ Р ИСО/МЭК 17799:2005. Международный стандарт ISO 27001 – ГОСТ Р ИСО/МЭК 27001:2006. Немецкий стандарт BSI. Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей». Стандарты

		информационной безопасности в Интернете. Отечественные стандарты в области защиты информации. Государственные органы в области защиты информации. Государственные стандарты по защите информации. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения». ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Специальные требования и рекомендации по технической защите конфиденциальной информации. Руководящие документы Гостехкомиссии (ФСТЭК) России. РД «Концепция защиты СВТ и АС от НСД к информации. РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации». РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации». РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Руководящие документы ФСТЭК по защите ключевых систем информационной инфраструктуры. Стандарты и рекомендации Банка России в области информационной безопасности. Модель угроз и модель нарушителя. Нормативные документы. Нарушитель информационной безопасности: определение, мотивы, классификация. Понятие и типы модели нарушителя. Модель нарушителя в соответствии с РД «Концепция защиты СВТ и АС от НСД к информации». Определение, цели и структура модели угроз. Разработкамодели угроз и модели нарушителя для информационной системы. Сертификация средств защиты информации. Нормативная база системы сертификации средств защиты информации. Основные термины. Цели сертификации. Система сертификации. Порядок сертификации. Сертификат соответствия. Схемы проведения сертификации средств защиты информации. Сертификация средств криптографической защиты информации. Основы проектирования программно-аппаратных комплексов обеспечения информационной безопасности. Этапы развития средств защиты информации (СЗИ). Особенности средств защиты информации, учитываемые при проектировании. Этапы разработки средств защиты информации. Основные принципы построения СЗИ. Принципы построения аппаратных СЗИ. Методы разработки программных и программно-аппаратных СЗИ. Обеспечение надежности программных и программно-аппаратных СЗИ.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости.

4.1.1. В ходе реализации дисциплины «Программно-аппаратные средства защиты информации» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Доклады с презентацией, опрос на практическом занятии
Тема 2	Доклады с презентацией, опрос на практическом занятии
Тема 3	Доклады с презентацией, опрос на практическом занятии
Тема 4	Доклады с презентацией, опрос на практическом занятии
Тема 5	Доклады с презентацией, опрос на практическом занятии

4.1.2. Зачет проводится в форме устного ответа на билеты (по 2 вопроса в билете).

4.2. Материалы текущего контроля успеваемости обучающихся

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется при опросе на практических занятиях, докладах с презентацией.

Тема 1. Защита программ и данных.

Вопросы для подготовки обучающихся к практическим занятиям

Основные способы НСД в локальном компьютере. Методы и средства защиты информации от НСД в локальном компьютере. Задачи и функции программно-аппаратных средств защиты компьютера. Традиционные методы, технологии и средства защиты информации в автоматизированной системе. Методы и средства ограничения доступа к компонентам компьютера. Дискреционный и мандатный принципы разграничения доступа. Методы аутентификации пользователей. Принцип действия, достоинства и недостатки аппаратных устройств на основе электронных (магнитных) идентификаторов. Принцип действия, достоинства и недостатки аппаратных устройств на основе биометрических характеристик субъекта. Защита от изменения и контроль целостности. Замкнутая программная среда. Регистрация событий (журналирование) в автоматизированной системе. Классификация разрушающих программных воздействий. Принципы работы антивирусных средств. Основные технологии и методы резервного копирования. Принципы и методы анализа и исследования программ. Методы защиты от изучения программ. Классификация и принципы действия технических методов защиты от несанкционированного копирования информации.

Тема 2. Защита в операционных системах

Вопросы для подготовки обучающихся к практическим занятиям

Защита операционных систем. Средства собственной защиты. Процедура идентификации и аутентификации. Контроль и управление доступом. Регистрация событий. Реализация механизмов безопасности на аппаратном уровне. Защита на уровне расширений BIOS. Защита на уровне загрузчиков операционной среды. Создание

защищенной операционной системы. Основные положения архитектуры микроядерных ОС. Микроядерная архитектура с точки зрения создания защищенных систем. Средства обеспечения безопасности в ОС семейств UNIX и Windows. Домены безопасности. Критерии защищенности операционной системы.

Тема 3. Защита в сетях

Вопросы для подготовки обучающихся к практическим занятиям
Основные каналы утечки информации при подключении к сетям общего пользования. Методы и средства защиты информации при подключении к сетям общего пользования. Протоколы аутентификации при удаленном доступе. Сканеры безопасности. Защита от анализаторов протоколов. Межсетевые экраны – эффективная технология сетевой защиты информации. Современные требования к межсетевым экранам. Классификация и технология VPN. Системы обнаружения вторжений. Управление криптографическими ключами и хранение ключевой информации. Концепция иерархии ключей.

Тема 4. Защита в СУБД.

Вопросы для подготовки обучающихся к практическим занятиям
Угрозы НСД, специфичные для СУБД. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Средства обеспечения защиты информации в СУБД: идентификация и проверка подлинности пользователей, управление доступом, поддержание целостности информации, организация аудита. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа. Модели безопасности, применяемые при построении защиты в СУБД. Ссылочная целостность, триггерная и событийная реализации правил безопасности. Транзакция и восстановление. Кластерная организация серверов баз данных. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных. Особенности применения криптографических методов. Функции администратора безопасности баз данных.

Тема 5. Нормативно-правовые основы применения, сертификации средств и систем защиты информации.

Вопросы для подготовки обучающихся к практическим занятиям
Основные зарубежные и отечественные стандарты в области информационной безопасности и их применение. Классификация автоматизированных систем в соответствии с руководящими документами. Классификации и модели угроз безопасности информации в АС, представленные в основных отечественных и зарубежных стандартах и нормативных документах. Модель нарушителя при локальном и удалённом НСД. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности. Влияние стандартов безопасности на проектирование и разработку программно-аппаратных средств защиты информации.

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-6	способен собирать детальную информацию для формализации требований пользователей заказчика	ПК-6.3	Способен документировать полученные данные на основании регламентов организации
ПК-7	способен проводить описание прикладных процессов и информационного обеспечения решения прикладных задач	ПК-7.1	Способен выбирать методы и средства описания прикладных процессов в решении прикладных задач
ПК-18	способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-18.2	ПК-18.2 Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС

4.3.2. Типовые оценочные средства

Промежуточный контроль проводится в форме зачета и предусматривает устный ответ на вопросы по билету.

Код и содержание этапа освоения компетенции	Результаты обучения	Оценочное средство
ПК-6.3	на уровне знаний: знать методы анализа предметной области информационных потребностей и формирования требований к информационной системе;	устный опрос
	на уровне умений: уметь проводить анализ предметной области, выявлять информационные потребности пользователей заказчика;	устный опрос
	на уровне навыков: обладать навыками применения методов и инструментальных средств описания и анализа требований пользователей заказчика.	устный опрос
ПК-7.1	на уровне знаний: знать теорию и средства проектирования структур данных, информационных процессов и информационного обеспечения решения прикладных задач;	устный опрос
	на уровне умений: уметь анализировать и описывать информационные процессы и	устный опрос

	информационное обеспечение решения прикладных задач;	
	на уровне навыков: иметь навыки применения современных инструментальных средств при описании и проектировании информационных процессов и информационного обеспечения решения прикладных задач.	устный опрос
ПК-18.2	на уровне знаний: знать виды угроз безопасности, методы и средства обеспечения информационной безопасности, подходы к организации ИТ - инфраструктуры;	устный опрос
	на уровне умений: уметь организовывать защиту информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);	устный опрос
	на уровне навыков: иметь навык обеспечения информационной безопасности и защиты информации, организации ИТ – инфраструктуры.	устный опрос

Перечень вопросов к зачету

1. Назначение и функции программно-аппаратных средств обеспечения безопасности. Цели и задачи курса.
2. Основные понятия и определения.
3. Эскалация привилегий.
4. Функции программно-аппаратных средств защиты информации.
5. Содержание и задачи процесса обеспечения информационной безопасности с использованием программно-аппаратных средств.
6. Методы защиты информации от несанкционированного доступа
7. Требования к специализированным средствам защиты информации от несанкционированного доступа.
8. Контроль целостности системного программного обеспечения и аппаратных средств. Организация виртуальных логических дисков.
9. Шифрование пользовательских виртуальных дисков.
10. Формирование ключевой информации.
11. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем
12. Средства обеспечения целостности составных частей компьютера.
13. Защита узлов и блоков компьютеров от несанкционированного доступа. Средства контроля доступа к рабочему месту пользователя.
14. Программные средства выявления фактов физического доступа к системному блоку и узлам автоматизированной системы.
15. Анализ уязвимости программного обеспечения автоматизированных систем
16. Понятие вредоносного кода. Программные закладки.
17. Классификация программных закладок. Предпосылки к внедрению программных закладок.
18. Уязвимости программного обеспечения.
19. Принципы построения политики безопасности. Уязвимости политики безопасности.
20. Человеческий фактор.
21. Сокрытие программных закладок.
22. Методы защиты от вредоносных программ
23. Сигнатурное и эвристическое сканирование. Аппаратные средства противодействия вредоносному коду.

24. Контроль целостности программного обеспечения. Мониторинг информационных потоков.
25. Изолированная программная среда.
26. Цифровая подпись исполняемого кода. Шифрование исполняемого кода.
27. Средства анализа уязвимостей.
28. Средства идентификация и аутентификации пользователей автоматизированных систем
29. Применение парольных систем.
30. Аутентификация с помощью физических предметов хранящихся у пользователя. Электронные ключи. Пластиковые карты.
31. Особенности идентификации и аутентификации с помощью биометрических характеристик пользователей.
32. Использование криптографических методов в системах аутентификации. Протоколы и алгоритмы аутентификации и идентификации пользователей в современных операционных системах ОС.

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание лекционного материала

Критериями оценки ответа обучающихся на лекционном занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки **«отлично»** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки **«хорошо»** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **«удовлетворительно»** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **«неудовлетворительно»** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3. Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине

Зачет принимается в устной форме, по билетам. Задание для зачета включает два теоретических вопроса. Оценка знаний обучающегося на зачете носит комплексный характер и определяется его:

- ответом на зачете;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на зачете оцениваются оценками: «зачтено», «незачтено». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

Оценивание студента на зачете по дисциплине «Программно-аппаратные средства защиты информации»

Оценка	Требования к знаниям
Зачтено	«Зачтено» выставляется обучающемуся, если он показал полные, глубокие и систематические знания, знакомство с дополнительной литературой, полный и правильный ответ, творческий подход в понимании и изложении учебного материала, полное выполнение мероприятий текущего контроля. Допустимо знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий промежуточного контроля и при ответе.
Незачтено	«Незачтено» выставляется обучающемуся, если он не выполнил предусмотренные программой задания, не отработал практические или лабораторные занятия, необходимые дополнительные занятия по соответствующей дисциплине, нарушил академические нормы, имеет существенные погрешности при выполнении мероприятий текущего контроля, допущены существенные ошибки при ответе, необходима некоторая дополнительная работа.

5. Методические указания для обучающихся по освоению дисциплины

5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего

обсуждения на практическом занятии. В случае необходимости следует обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 настоящей программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

– использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;

– представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;

– грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.2.1. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

5.3. Методические рекомендации по подготовке к зачету по дисциплине

Ответ на зачете предусматривает устный ответ на теоретические вопросы.

При подготовке к зачету обучающийся обращается к пройденному материалу, сосредоточенному в конспектах лекций, учебниках и других источниках информации. Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно-новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено в лекциях и на семинарских занятиях.

Зачет как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

• что и как запоминать при подготовке к экзамену;

• по каким источникам и как готовиться;

• на чем сосредоточить основное внимание;

• каким образом в максимальной степени использовать программу курса;

• что и как записать, а что выучить дословно и т. п.

На зачете, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными научными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом зачете. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для зачета.

Оптимальным для подготовки к зачеу является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к зачету по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к зачету следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, иллюстрированные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает.

В то же время подготовка по одним конспектам лекций недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и уточняющих вопросов на зачете. Они, как правило, задаются или помимо теоретического вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет, включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. — М.: Издательство Юрайт, 2017. — 312 с. — (Серия: Специалист). — ISBN 978-5-9916-9043-0.

2. Креопалов В.В. Технические средства и методы защиты информации. Практическое пособие - М.: Евразийский открытый институт, 2011. - 278 с. - 978-5-374-00507-3. Режим доступа: http://biblioclub.ru/index.php?page=book&id=90753

6.2. Дополнительная литература

1. Платонов В.В. Программно-аппаратные средства защиты информации: учебник — М.: Издательство Академия, 2013. - 336 с. - (Серия: Специалист). - ISBN 978-5-9916-9043-0.

2. Хорев П.Б. Программно-аппаратная защита информации: Учебное пособие. Гриф МО РФ — **М.: Издательство Инфра-М, Форум, 2017. — 352 с. — ISBN** 978-5-00091-004-7
3. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин М.В. Рудановский. - М.: Флинта, 2011. - 224 с. - 978-5-9765-1274-0. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93351

6.3. Нормативные правовые документы.

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации». Статья 16. Защита информации. СПС Консультант.
2. Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности». СПС Консультант.
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». СПС Консультант.
4. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». СПС Консультант.
5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». СПС Консультант.
6. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». СПС Консультант.
7. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации». СПС Консультант.
8. Федеральный закон от 21.07.93 № 5486–1 «О государственной тайне» http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156018
9. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=160225
10. Федеральный закон от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи» http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=165011

6.4. Интернет-ресурсы

- академические электронно-библиотечные системы учебной литературы.
- база научно-технической информации ВИНИТИ РАН
- доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, math-net.ru
-среды разработки на языках C#, C++, Pascal, Java;

6.5. Иные источники.

Не предусмотрены

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Название	Наименование оборудования	Перечень

лаборатории/класса, оснащенного необходимым, в соответствии с требованиями ФГОС/ СУОС, оборудованием		**лицензионного программного обеспечения**
учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Рабочие места студентов: столы и стулья – соответственно количеству студентов. Рабочее место для инвалида и лиц с ОВЗ: парта с телескопической столешницей на электромеханическом приводе - 1 шт., кресло-коляска для инвалидов 18" - 1 шт., индукционная петля - 1 шт., компьютер с версией для слабовидящих - 1 шт., кнопка вызова сотрудников - 1 шт. Рабочее место преподавателя: стол – 1 шт., стул – 1 шт, кафедра - 1 шт. Доска меловая и маркерная. Экран, ноутбук Lenovo ideapad 100/15, проектор	Мультимедийный проектор КонсультантПлюс
информационно-аналитическая лаборатория - учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций	Рабочие места: столы компьютерные – в соответствии с количеством студентов, кресло Престиж Profi -B-20 Самба бордо в рубчик - 15 шт., подставка для ног Fellowes FS-48121 Standard черный - 15 шт. Рабочее место преподавателя: стол компьютерный - 1 шт., стул - 1 шт. Доска меловая или маркерная Персональные компьютеры	Мультимедийный проектор КонсультантПлюс
библиотека - помещение для самостоятельной работы	Рабочие места: столы и стулья. Рабочее место преподавателя: стол – 1 шт., стул - 1 шт., кафедра библиотечная - 1 шт. Телефон – 1 шт., цифровой многофункциональный копир - 1 шт., копировальный аппарат МФУ – 1 шт., принтер - 1 шт., сканер – 1 шт. Шкаф – 7 шт, стеллаж-33 шт, библиотечная стойка – 2 шт., стенд – 2 шт. Меловая или маркерная доска. Персональные компьютеры	Мультимедийный проектор КонсультантПлюс

Программное обеспечение:
В процессе лекционных и семинарских занятий используется следующее программное обеспечение:

- программы, обеспечивающие доступ в сеть Интернет (например, «Google chrome») и локальную сеть Академии;
- программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»).

Информационные справочные системы:
Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: http://www.consultant.ru/
Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: http://www.garant.ru/