Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ
И.о. декана радиотехнического факультета
_____ / В.А. Баженов /
27 июня 2018

Рабочая программа дисциплины

Программно-аппаратные средства обеспечения информационной безопасности

Базовой части образовательной программы
по специальности

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы

«Обеспечение информационной безопасности
распределённых информационных систем»

Факультет/институт: Радиотехнический (РТФ)

Кафедра информационной безопасности

Калининград 2018 г.

Визирование РПД для исполнения в очередном учебном году

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«27» июня 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2018 – 2019 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «14» июня 2018 г. № 9

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«____» _____ 2019 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2019 – 2020 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «___» _____2019 г. №

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

1. Цель освоения дисциплины.

1.1. Цель изучения дисциплины.

- обучить студентов принципам построения систем защиты информации (СЗИ) в операционных системах (ОС), вычислительных сетях (ВС) и системах управления базами данных (СУБД);

- пользоваться полученными знаниями и практическими навыками при разработке курсовых и дипломных работ.

1.2. Задачи изучения дисциплины.

Изучить:

- методы и средства ограничения доступа к компонентам ВС;

- методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям;

- методы и средства хранения ключевой информации;

- задачи и технологию сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности;

- способы встраивания средств защиты в программное обеспечение;

- цели и задачи защиты информации в сетях передачи данных;

- основные нормативные правовые акты и методические документы по защите от НСД.

1.3. Предметом изучения дисциплины являются следующие объекты:

Программные, программно-аппаратные средства обеспечения информационной безопасности автоматизированных информационных систем.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.
ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий	знать: принципы построения современных программных, технических средств и информационных технологий; принципы эксплуатации и ограничения современных программных, технических средств и информационных технологий уметь: уметь определять особенности современных программных, технических средств и информационных технологий при их изучении; эксплуатировать современные программных, технических средств и информационных технологий владеть: методикой эксплуатации современные программных, технических средств и информационных технологий.

ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	знать: методики поиска, изучения, обобщения и систематизации научно-технической информации, виды нормативных и методических материалов в сфере профессиональной деятельности уметь: осуществлять поиск и обобщать, систематизировать научно-техническую информацию в области информационной защиты, использовать нормативные и методические материалы в сфере профессиональной деятельности владеть: методикой поиска, изучения, обобщения и систематизации научно-технической информации
ПК-3	способностью проводить анализ защищенности автоматизированных систем	**знать**: методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера **уметь:** определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники. Оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ). Создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем **владеть:** методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать: классы угроз распределенной системы обработки информации; методику поиска актуальных уязвимостей распределенной системы; порядок создания модели нарушителя; определение базовой модели нарушителя; неформальной модели нарушителя; типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах; определение категории нарушителя; типологию нарушителей по характеру

		поведения Уметь: установить приоритеты целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз; создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации Владеть: установить приоритеты целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз. создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	знать: методологию оценку риска; оценку ущерба от реализацию угроз; групп оценки риска; этапы оценки риска: определение степени детализации, идентификация и оценка ценностей, идентификация угроз и определение их вероятности; измерение риска; выбор мер и средств защиты в соответствии с уровнем риска; внедрение и тестирование средств защиты; утверждение остаточного риска; методику оценки потенциально возможных угроз информационной системы и средств защиты: оценка ущерба от угроз безопасности информации, показатели предотвращенного ущерба; методики оценки угроз уметь: выбирать методику оценки угроз; производить оценку ущерба от угроз безопасности информации; производить оценки потенциально возможных угроз информационной системы и средств защиты владеть: методикой идентификации и оценки угроз; методикой оценки риска; методикой определения вероят-

		ности угроз, ;методикой оценки ущерба в зависимости от применяемы средств защиты
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	знать: Способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий; принципы определения эффективности предложенных решений с учетом снижения рисков автоматизированной системы. уметь: Определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации. владеть: Методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей; средствами защиты информации в процессе хране-

		ния и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	знать: политику информационной безопасности автоматизированной системы уметь: разрабатывать политику информационной безопасности автоматизированной системы владеть: способностью разрабатывать политику информационной безопасности автоматизированной системы
ПК-14	способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	знать: принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для проверки проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; методы определения стойкости парольной защиты; механизмы активного и пассивного анализа уязвимостей; определять эффективность применяемых программно-аппаратных, криптографических и технических средств защиты информации в зависимости степень риска и вероятность осуществления НСД; принципы контроля данных при передачи информации по прободным и беспроводным каналам связи при использовании криптографических протоколов; языки описания уязвимостей и проверок; теоретико-графовые модели комплексной оценки защищенности распределенных ресурсов уметь: применять сканеры безопасности в пассивном и активном режиме; производить аудит распределенных систем; анализировать результаты сканирования; использовать

		снифферы для анализа потока передаваемой информации; рассчитывать степень защищенности передаваемой информации; определять степень стойкости паролей; применять системы анализа защищенности; системы анализа рисков владеть: программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; владеть методами сканирования: проверка заголовков, активные зондирующие проверки, имитация атак; методами и средствами проверки стойкости парольной защиты; программным обеспечением и методиками анализа защищенности распределенных ресурсов; программным обеспечением и методиками анализа рисков
ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	знать: принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения уметь: применять принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; производить аудит распределенных систем; анализировать результаты сканирования владеть: методиками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем, аудита распределенных систем; анализа результатов сканирования

ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	знать: методы инструментального мониторинга защищенности информации; способы и средства выявления каналов утечки информации уметь: проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации владеть: методами инструментального мониторинга защищенности информации; способами и средствами выявления каналов утечки информации
ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	знать: методы инструментального мониторинга защищенности информации; способы и средства выявления каналов утечки информации уметь: проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации владеть: методами инструментального мониторинга защищенности информации; способами и средствами выявления каналов утечки информации
ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Знать: методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности Уметь: обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности Владеть: методами обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	знать: способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановление ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; способы защиты программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий. уметь: применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы; восстанавливать ресурсы автоматизированной системы, их работоспособность при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; применять методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; применять методы и средства хранения ключевой информации; осуществлять защиту программ от изучения, встраивать средства защиты в программное обеспечение; осуществлять защиту от разрушающих программных воздействий. владеть: методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; методикой восстановления ресурсов автоматизированной системы, их работоспособности при возникновении нештатных ситуаций; методами и средствами ограничения доступа к компонентам вычислительных систем; методикой применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; методикой применения методов и средств хранения ключевой информации; методикой защиты программ от изучения, методикой встраивания средств защиты в программное обеспечение; методикой защиты от разрушающих программных воздействий.

ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	знать: способы и механизмы администрирования подсистем информационной безопасности, критерии эффективности применения СЗИ уметь: администрировать подсистем информационной безопасности, применять критерии эффективности применения СЗИ автоматизировать работу по административной настройке СЗИ от НСД владеть: способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	знать: виды политик безопасности, способы мониторинга и аудита уметь: настраивать механизмы политик безопасности, способы мониторинга и аудита в ОС владеть: механизмами администрирования, встроенными в ОС
ПК-28	способностью управлять информационной безопасностью автоматизированной системы	знать: способы и механизмы управления информационной безопасностью автоматизированной системы уметь: примять способы и механизмы управления информационной безопасностью автоматизированной системы владеть: способами, механизмами способы и механизмы управления информационной безопасностью автоматизированной системы

Таблица 2 - Этапы формирования компетенций

Коды компетенций	Этапы формирования компетенций (разделы программы)

ОПК-8, ПК-1, ПК-3, ПК-4, ПК-5, ПК-6, ПК-11, ПК-14, ПК-15, ПК-17, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28	Тема 1. Надежность информации. Элементы информационной базы автоматизированной системы обработки данных. Уязвимость информации. Тема 2. Основные принципы создания автоматизированных систем. Технологические особенности схем автоматизированной обработки данных. Классы автоматизированных систем (АИС) и их подсистем, подлежащих защите. Критичность подсистем АИС. Тема 3. Функциональные требования по защите автоматизированных систем. Классификация аппаратных средств защиты. Классификация программных средств защиты. Тема 4. Идентификация и аутентификация субъекта доступа. Концепция диспетчера доступа. Ядро безопасности. Тема 5. Методы и средства ограничения доступа к компонентам вычислительных систем. Применение дискреционной политики безопасности на основе методов СЗИ. Тема 6. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Тема 7. Методы и средства организации хранения и переработки ключевой информации. Методы резервирования ключевой информации. Тема 8. Классификация компьютерных вирусов. Классификация методов и средств борьбы с компьютерными вирусами. . Тема 9. Условия безопасной работы компьютерной системы и технология обнаружения заражения вирусами. Методики распознавания и извлечения вредоносных программ. Тема 10. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Тема 11. Источники формирования дестабилизирующих факторов. Контроль целостности и системные вопросы защиты программ и данных. Использование СЗИ для контроля целостности. Организация контроля. Выявление ресурсов подлежащих контролю. Построение изолированной программной среды. Тема 12. Цели и задачи защиты информации в сетях передачи данных. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях. Тема 13 Сервис безопасности. Методы цифровой подписи данных, передаваемых в сети. Контроль передаваемых данных. Тема 14. Система защиты локальной вычислительной сети. Межсетевые экраны (МЭ). Построение и принцы работы МЭ. Применение правил фильтрации МЭ при обработки сетевых пакетов в сети. Тема 15. Защита процессов переработки информации в Интернете и Интранете. Системы блокирование атак. Отслеживание удаленного сканирования ресурсов сети. Тема 16. Системы активного аудита. Практика применения программ аудита NESSUS. Аудит АИС. Тема 17.Правовые методы защиты процессов переработки информации. Требования и рекомендации ФСТЕК России по защите информации, обрабатываемой средствами вычислительной техники. Последовательность процедур сертификации. Тема 18. Классификация автоматизированных систем. Показатели защищенности СВТ. Критерии оценки надежности автоматизиро-

	ванных систем.

Таблица 3 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	- методы и средства ограничения доступа к компонентам ВС; - методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; - методы и средства хранения ключевой информации; - задачи и технологию сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; - способы встраивания средств защиты в программное обеспечение; - цели и задачи защиты информации в сетях передачи данных; - основные нормативные правовые акты и методические документы по защите от НСД.
уметь	- организовывать защиту программ от изучения; - производить защиту от разрушающих программных воздействий; - производить защиту программ от изменений; - осуществлять контроль целостности программ и построение изолированной программной среды.
владеть	- средствами контроля информационной целостности; - средствами защиты автоматизированного комплекса от несанкционированного доступа; - средствами борьбы с вирусами и вредоносными закладками.

3. Место дисциплины в структуре образовательной программы

Место дисциплины в структуре ООП:

Б2.Б.30 Базовая часть Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

Требования к предварительной подготовке обучающегося:

Перечень дисциплин, усвоение которых необходимо для изучения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности»: «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Безопасность операционных систем», «Правовое обеспечение информационной безопасности».

Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

"Комплексное обеспечение информационной безопасности автоматизированных систем".

4. Содержание дисциплины

Тема 1. Надежность информации. Элементы информационной базы автоматизированной системы обработки данных. Уязвимость информации.

Тема 2. Основные принципы создания автоматизированных систем. Технологические особенности схем автоматизированной обработки данных. Классы автоматизированных систем (АИС) и их подсистем, подлежащих защите. Критичность подсистем АИС.
Тема 3. Функциональные требования по защите автоматизированных систем. Классификация аппаратных средств защиты. Классификация программных средств защиты.
Тема 4. Идентификация и аутентификация субъекта доступа. Концепция диспетчера доступа. Ядро безопасности.
Тема 5. Методы и средства ограничения доступа к компонентам вычислительных систем. Применение дискреционной политики безопасности на основе методов СЗИ.
Тема 6. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
Тема 7. Методы и средства организации хранения и переработки ключевой информации. Методы резервирования ключевой информации.
Тема 8. Классификация компьютерных вирусов. Классификация методов и средств борьбы с компьютерными вирусами. .
Тема 9. Условия безопасной работы компьютерной системы и технология обнаружения заражения вирусами. Методики распознавания и извлечения вредоносных программ.
Тема 10. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение.
Тема 11. Источники формирования дестабилизирующих факторов. Контроль целостности и системные вопросы защиты программ и данных. Использование СЗИ для контроля целостности. Организация контроля. Выявление ресурсов подлежащих контролю. Построение изолированной программной среды.
Тема 12. Цели и задачи защиты информации в сетях передачи данных. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.
Тема 13 Сервис безопасности. Методы цифровой подписи данных, передаваемых в сети. Контроль передаваемых данных.
Тема 14. Система защиты локальной вычислительной сети. Межсетевые экраны (МЭ). Построение и принцы работы МЭ. Применение правил фильтрации МЭ при обработки сетевых пакетов в сети.
Тема 15. Защита процессов переработки информации в Интернете и Интранете. Системы блокирование атак. Отслеживание удаленного сканирования ресурсов сети.
Тема 16. Системы активного аудита. Практика применения программ аудита NESSUS. Аудит АИС.
Тема 17.Правовые методы защиты процессов переработки информации. Требования и рекомендации ФСТЕК России по защите информации, обрабатываемой средствами вычислительной техники. Последовательность процедур сертификации.
Тема 18. Классификация автоматизированных систем. Показатели защищенности СВТ. Критерии оценки надежности автоматизированных систем. Заключение.

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации

Таблица 1 - Объем (трудоемкость освоения) и структура дисциплины, формы аттестации для очной формы обучения

Номер и наименование разделов и тем	Объем учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СРС	Контроль	Всего
Семестр - 8 (144 час.; 4 ЗЕТ).						
Тема 1. Надежность информации. Элементы информационной базы автоматизированной системы обработки данных. Уяз-	4					4

вимость информации.						
Тема 2. Основные принципы создания автоматизированных систем. Технологические особенности схем автоматизированной обработки данных. Классы автоматизированных систем (АИС) и их подсистем, подлежащих защите. Критичность подсистем АИС.	4			18		22
Тема 3. Функциональные требования по защите автоматизированных систем. Классификация аппаратных средств защиты. Классификация программных средств защиты.	4	4		12		18
Тема 4. Идентификация и аутентификация субъекта доступа. Концепция диспетчера доступа. Ядро безопасности. .	4	4				8
Тема 5. Методы и средства ограничения доступа к компонентам вычислительных систем. Применение дискреционной политики безопасности на основе методов СЗИ.	4	4				8
Тема 6. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	4	4		21		29
Тема 7. Методы и средства организации хранения и переработки ключевой информации. Методы резервирования ключевой информации.	4	4				8
Тема 8. Классификация компьютерных вирусов. Классификация методов и средств борьбы с компьютерными вирусами.	4	8				12
Тема 9. Условия безопасной работ компьютерной системы и технология обнаружения заражения вирусами. Методики распознавания и извлечения вредоносных программ.	2	6		25		33
Подготовка к сдаче и сдача зачета						
Всего в семестре	34	34		76		144
Семестр - 9 (144 час; 4 ЗЕТ)						
Тема 10. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение.	8	12				20
Тема 11. Источники формирования дестабилизирующих факторов. Контроль	8	10		2		20

целостности и системные вопросы защиты программ и данных. Использование СЗИ для контроля целостности. Организация контроля. Выявление ресурсов подлежащих контролю. Построение изолированной программной среды.						
Тема 12. Цели и задачи защиты информации в сетях передачи данных. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.	4	4				8
Тема 13 Сервис безопасности. Методы цифровой подписи данных, передаваемых в сети. Контроль передаваемых данных.	4	2				6
Тема 14. Система защиты локальной вычислительной сети. Межсетевые экраны (МЭ). Построение и принцы работы МЭ. Применение правил фильтрации МЭ при обработки сетевых пакетов в сети.	4	4				8
Тема 15. Защита процессов переработки информации в Интернете и Интранете. Системы блокирование атак. Отслеживание удаленного сканирования ресурсов сети.	4	4				8
Тема 16. Системы активного аудита. Практика применения программ аудита NESSUS. Аудит АИС.	4	8		2		14
Тема 17.Правовые методы защиты процессов переработки информации. Требования и рекомендации ФСТЕК России по защите информации, обрабатываемой средствами вычислительной техники. Последовательность процедур сертификации.	4			2		6
Тема 18. Классификация автоматизированных систем. Показатели защищенности СВТ. Критерии оценки надежности автоматизированных систем. Заключение.	4			2		6
Выполнение КР				12	36	48
Подготовка к сдаче и сдача экзамена						
Всего в семестре	44	44		20	36	144
Итого по дисциплине	78	78		96	36	288

ЛЗ – лабораторные занятия,
ПЗ – практические занятия,
СРС – самостоятельная работа студента,
КР – курсовая работа,
КП – курсовой проект.

6. Лабораторные занятия (работы)

Таблица 2 - Лабораторные по очной форме обучения

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов ЛЗ
Семестр – 8 (34 час.).			
1.	Тема 3.	Выявления возможных каналов НСД.	4
2.	Тема 4.	Идентификация и аутентификация субъекта доступа в СЗИ	4
3.	Тема 5	Применение методов и средств ограничения доступа к компонентам вычислительных систем в СЗИ.	4
4.	Тема 6	Программирование под HASP с использованием API-функций.	4
5.	Тема 7	Применение методов и средств организации хранения и переработки ключевой информации в СЗИ.	4
6.	Тема 8	Определение жизненно цикла вредоносных программ и извлечение компьютерного вируса средствами антивирусных программ и утилит.	4
7.	Тема 8	Особенности извлечения компьютерного вируса типа «червь»	4
8.	Тема 9	Исследование функциональных особенностей «Macro-вирусов»	4
9.	Тема 9.	Обнаружение клавиатурных шпионов (keylogger).	2
Всего за семестр:			34
Семестр – 9 (44 час.).			
1.	Тема 10.	Исследование моделей защит ПО. Защита от отладчиков.	4
2.	Тема 10.	Исследование моделей защит ПО. Защита от дизассемблеров. Изучение средств динамического исследования программ на примере отладчика Olly Debugger.	8
3.	Тема 11.	Организация контроля и построение изолированной программной среды средствами СЗИ.	6
4.	Тема 11.	Контроль целостности и системные вопросы защиты программ и данных средствами СЗИ.	4
5.	Тема 12.	Изучение функций СЗИ "Блокхост-сеть К".	4

6.	Тема 13.	Методы цифровой подписи данных, передаваемых в сети.	2
7.	Тема 14.	Программно-аппаратный комплекс доверенной загрузки "Блок-хост-МДЗ.	4
8.	Тема 15.	Применение Систем обнаружения вторжения.	4
9.	Тема 16	Применение программ аудита.	4
10.	Тема 16	Методы цифровой подписи данных, передаваемых в сети.	4
Всего за семестр:			44
Итого по дисциплине			78

7. Практические занятия

Практические занятия по дисциплине учебным планом не предусмотрены.

8. Самостоятельная работа студента

Таблица 3 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
Семестр – 8 (76 час.)			
1.	Угрозы безопасности автоматизированных систем обработки данных. Методы идентификации и установления подлинности субъектов и различных объектов. Состав и структура методов и систем обеспечения информационной безопасности. Методы и средства нейтрализации угроз	18	Текущий контроль: опрос, тест
2.	Система управления доступом и организация автоматизированной системы контроля доступом (АСКД). Способы аутентификации пользователей.	12	
3.	Парольные методы проверки подлинности пользователей. Методы контроля целостности программ и данных. Методы и средства предотвращения несанкционированного доступа в автоматизированных системах. Методы и средства организации обеспечения хранения и переработки ключевой информации.	21	

4	Средства борьбы с вирусами и вредоносными закладками. Характеристика программной защиты ПК Ad-Aware. Загрузочные и файловые вирусы. Защита программных средств от несанкционированного использования и копирования. Вредоносные программы и их классификация.	25	
Всего за семестр:		76	
Семестр – 9 (20 час.)			
5.	Особенности применения следующих комплексов: Программно-аппаратный комплекс «Страж NT» Программно-аппаратный комплекс «Strong Disk»Система защиты информации «Dallas Lock 7.0» Программно-аппаратный комплекс «Аккорд-NT/2000» Система защиты информации «Secret Disk».Система защиты информации «Secret Net 5.0	2	Текущий контроль: Опрос
6.	Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.	2	
7.	Руководящий документ Гостехкомиссии при Президенте РФ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». /Ср/	2	
8	ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний». ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированно доступа к информации». Государственная техническая комиссия при президенте РФ специальные требования и рекомендации по технической защите конфиденциальной информации 2001г.	2	
9	Выполнение КП	12	
Всего за семестр:		20	
Итого по дисциплине		96	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

Таблица 4 – Основная учебная литература

Авторы, составители	Заглавие	Издательство, год	Колич-во
Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: учебное пособие	М. : ИД "Форум" ; М. : ИНФРА-М, 2013. - 416 с.	20

Таблица 5 – Дополнительная учебная литература

Автор(ы)	Заглавие	Издательство, год.	Колич-во
Жестовский А.Г.	Программно-аппаратные средства обеспечения информационной безопасности: Методические указания по выполнению курсовой работы	Калининград: БГАРФ, 2009	30

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Программное обеспечение

1.Программное обеспечение по Договору о сотрудничестве с ООО "Газинформсервис

– СЗИ Блокхост-МДЗ. Договор о сотрудничестве №012 ООО "Газинформсервис", артикул БХМДЗ-4М-10-49 "Блокхост-МДЗ" /лицензии:26 шт./ Дата: 14.06.2018 г. (срок действия: три года);

– СЗИ Блокхост-сеть 2.0. Договор о сотрудничестве №012 ООО "Газинформсервис", артикул БХС2.0-АВ-10-49 "Блокхост-сеть 2.0" /лицензии:26 шт./ Дата: 14.06.2018 г.(срок действия: три года);

– ПК Efros Config Inspector 3.0 Premium Клиент сервера управления среды виртуализации. Договор о сотрудничестве №012 ООО "Газинформсервис", артикул ECIP3.0-CLI-VCS "Efros Config Inspector 3.0" /лицензии:26 шт./ Дата: 14.06.2018 г.(срок действия: три года);

– ПК Efros Config Inspector 3.0 Premium. Сервер. Договор о сотрудничестве №012 ООО "Газинформсервис"

– артикул ECIP3.0-CLI-VCS "Efros Config Inspector 3.0" /лицензии:26 шт./ Дата: 14.06.2018 г.(срок действия: три года).

2.Программное обеспечение по Договору о сотрудничестве с ООО ООО "Конфидент"

– СЗИ DALLAS LOCK 8.0-К. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:26 шт./ Дата: 01.11.2018 г.(срок действия: три года);

– СЗИ DALLAS LOCK 8.0-К. Сервер безопасности. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:1 шт./ Дата: 01.11.2018 г.(срок действия: три года);

– СЗИ DALLAS LOCK 8.0-С. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:26 шт./ Дата: 01.11.2018 г.(срок действия: три года)

– СЗИ DALLAS LOCK 8.0-С. Сервер безопасности. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:1 шт./ Дата: 01.11.2018 г.(срок действия: три года).

3.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

4.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом)

Интернет-ресурсы

Интернет-ресурсы, применяемые при изучении:

1. http://www.intuit.ru/
2. http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/
3. http://eLIBRARY.RU (Научная лицензионная библиотека eLIBRARY.RU договор №673-03/2017К от 23. 03.207г., бессрочно)

11. Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебная аудитория № 441.

Состав оборудования: столы учебные – 15 шт., стол преподавательский – 1 шт., стулья учебные – 30 шт., стул преподавательский – 1 шт., трибуна – 1 шт., экран раздвижной PROJECTA – 1 шт.; доска магнитно-маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды: «Комплекс средств автоматизации деятельности оперативного персонала пункта централизованной охраны», «Требования и нормы проектирования по защите объектов от преступных посягательств». Специализированные стенды: СКУД «Стилпост»; «СИНЕРГЕТ» (цифровая система видеонаблюдения и аудиорегистрации).

Используется лицензионное программное обеспечение Microsoft Desktop Education, Microsoft Office 2016, Kaspersky Total Space Security Russian Edition.

11.1.2. Материально-техническое обеспечение для лабораторных занятий

Для проведения лабораторных занятий используется лаборатория технической защиты информации № 439.

Состав оборудования: столы учебные – 12 шт., стол преподавательский – 1 шт., стулья учебные – 17 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.

Компьютеры (системный блок, монитор, мышка, клавиатура), с установленным лицензионным программным обеспечением:

1.Программное обеспечение по Договору о сотрудничестве с ООО "Газинформсервис

– СЗИ Блокхост-МДЗ. Договор о сотрудничестве №012 ООО "Газинформсервис", артикул БХМДЗ-4М-10-49 "Блокхост-МДЗ" /лицензии:26 шт./ Дата: 14.06.2018 г. (срок действия: три года);

– СЗИ Блокхост-сеть 2.0. Договор о сотрудничестве №012 ООО "Газинформсервис", артикул БХС2.0-АВ-10-49 "Блокхост-сеть 2.0" /лицензии:26 шт./ Дата: 14.06.2018 г.(срок действия: три года);

– ПК Efros Config Inspector 3.0 Premium Клиент сервера управления среды виртуализации. Договор о сотрудничестве №012 ООО "Газинформсервис", артикул ECIP3.0-CLI-VCS "Efros Config Inspector 3.0" /лицензии:26 шт./ Дата: 14.06.2018 г.(срок действия: три года);

– ПК Efros Config Inspector 3.0 Premium. Сервер. Договор о сотрудничестве №012 ООО "Газинформсервис"

– артикул ECIP3.0-CLI-VCS "Efros Config Inspector 3.0" /лицензии:26 шт./ Дата: 14.06.2018 г.(срок действия: три года).

2.Программное обеспечение по Договору о сотрудничестве с ООО ООО "Конфидент"

– СЗИ DALLAS LOCK 8.0-К. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:26 шт./ Дата: 01.11.2018 г.(срок действия: три года);

– СЗИ DALLAS LOCK 8.0-К. Сервер безопасности. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:1 шт./ Дата: 01.11.2018 г.(срок действия: три года);

– СЗИ DALLAS LOCK 8.0-С. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:26 шт./ Дата: 01.11.2018 г.(срок действия: три года)

– СЗИ DALLAS LOCK 8.0-С. Сервер безопасности. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:1 шт./ Дата: 01.11.2018 г.(срок действия: три года).

3.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

4.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом).

Для проведения лабораторных занятий используются компьютерный класс № 248.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютеры (системный блок, монитор ASUS, мышка, клавиатура), с установленным лицензионным программным обеспечением: Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

11.1.3. Материально-техническое обеспечение для самостоятельной работы

Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12.Фонд оценочных средств для проведения аттестации по дисциплине.

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств для аттестации по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности».

13. Особенности преподавания и освоения дисциплины

13.1 Под образовательными технологиями будем понимать пути и способы формирования компетенций. В рамках дисциплины предусмотрены:

- лекции;
- лабораторные занятия, во время которых отрабатываются практические навыки, обсуждаются вопросы лекций, домашних заданий, проводятся контрольные и самостоятельные работы и т.д.;
- самостоятельная работа студентов, включающая усвоение теоретического материала, подготовку к практическим занятиям, выполнение индивидуальных заданий, курсовой работы, работа с учебниками, иной учебной и учебно-методической литературой, подготовка к текущему контролю успеваемости, к экзамену;
- тестирование по отдельным темам дисциплины;
- консультирование студентов по вопросам учебного материала.

13.2 Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

14. Методические указания по освоению дисциплины

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая *(*повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей):
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;

- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
- подготовка курсовых и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

15. Сведения о рабочей программе и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и соответствует учебному плану, утвержденному «31» января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор(ы) программы:
ст. преподаватель кафедры информационной безопасности _____ /В.В.Подтопельный/

Программа дисциплины рассмотрена и одобрена на заседании кафедры «Информационная безопасность» (протокол № 9 от 14 июня 2018 г.)

Зав. кафедрой информационной безопасности _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета (протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ / Жестовский А.Г.