Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

УТВЕРЖДАЮ
Первый проректор
С.В. Нотова
(подпись, расшифровка подписи)
"26" февраля 2021 г.

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2021

1 Общие положения

Целью государственной итоговой аттестации является установление соответствия результатов освоения обучающимися образовательной программы, разработанной в Оренбургском государственном университете соответствующим требованиям Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) и оценки уровня подготовленности выпускника к самостоятельной профессиональной деятельности.

В результате освоения образовательной программы обучающийся должен овладеть следующими компетенциями:

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
универсальными компетенциями (УК):			
УК-1	**Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	+	+
	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач		+
	УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников	+	+
	УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте		+
	УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач		+
	УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного аппарата		+
	УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий		+
УК-2	**Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**		+
	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта		+
	УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности		+
	УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта		+
	УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе оптимальных способов их		+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
	достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов		
УК-3	**Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде**		+
	УК-3-В-1 Понимает эффективность использования стратегии командного сотрудничества для достижения поставленной цели, определяет свою роль в команде		+
	УК-3-В-2 Генерирует идею, выбирает направление развития ее в проекте с учетом видовых характеристик и осуществляет социальное взаимодействие посредством распределения проектных ролей в команде		+
УК-4	**Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)**		+
	УК-4-В-1 Выбирает на государственном и иностранном (-ых) языках коммуникативно приемлемый стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами		+
	УК-4-В-2 Ведет деловую коммуникацию в письменной и электронной форме, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках		+
УК-5	**Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах**		+
	УК-5-В-1 Находит и использует необходимую для саморазвития и взаимодействия с другими информацию о культурных особенностях и традициях различных социальных групп		+
	УК-5-В-2 Демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России в контексте мировой истории и культурных традиций мира, включая мировые религии, философские и этические учения		+
	УК-5-В-3 Конструктивно взаимодействует с людьми различных категорий с учетом их социокультурных особенностей в целях успешного выполнения профессиональных задач и социальной интеграции		+
УК-6	**Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни**		+
	УК-6-В-1 Понимает важность планирования целей собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста,		+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
	временной перспективы развития деятельности и требований рынка труда		
	УК-6-В-2 Реализует намеченные цели с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда		+
	УК-6-В-3 Демонстрирует интерес к учебе и использует предоставляемые возможности для приобретения новых знаний и навыков		+
	УК-6-В-4 Критически оценивает эффективность использования времени при решении поставленных задач		+
УК-7	**Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности**	**+**	**+**
	УК-7-В-1 Соблюдает нормы здорового образа жизни, используя основы физической культуры для осознанного выбора здоровьесберегающих технологий на всех жизненных этапах развития личности	+	+
	УК-7-В-2 Выбирает рациональные способы и приемы профилактики профессиональных заболеваний, психофизического и нервноэмоционального утомления на рабочем месте		+
УК-8	**Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов**		**+**
	УК-8-В-1 Формирует культуру безопасного и ответственного поведения в повседневной жизни и профессиональной деятельности, обеспечивая безопасные и/или комфортные условия жизнедеятельности, труда на рабочем месте, в т.ч. с помощью средств защиты		+
	УК-8-В-2 Использует приемы первой помощи, методы защиты в условиях чрезвычайных ситуаций и военных конфликтов		+
	УК-8-В-3 Идентифицирует угрозы (опасности) природного и техногенного происхождения для жизнедеятельности человека и природной среды		+
	УК-8-В-4 В случае возникновения чрезвычайных ситуаций и военных конфликтов применяет методы защиты жизнедеятельности человека, принимает участие в спасательных и неотложных аварийно-восстановительных мероприятиях		+
УК-9	**Способен принимать обоснованные экономические решения в различных областях жизнедеятельности**		**+**
	УК-9-В-1 Выявляет и обосновывает сущность, закономерности экономических процессов, осознает их природу и связь с другими процессами; понимает		+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
	содержание и логику поведения экономических субъектов; использует полученные знания для формирования собственной оценки социально-экономических проблем и принятия аргументированных экономических решений в различных сферах жизнедеятельности		
	УК-9-В-2 Взвешенно осуществляет выбор оптимального способа решения финансово-экономической задачи, с учетом интересов экономических субъектов, ресурсных ограничений, внешних и внутренних факторов		+
	УК-9-В-3 Понимает последствия принимаемых финансово-экономических решений в условиях сформировавшейся экономической культуры; способен, опираясь на принципы и методы экономического анализа, критически оценить свой выбор с учетом области жизнедеятельности		+
УК-10	**Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности**		**+**
	УК-10-В-1 Понимает сущность экстремизма, терроризма, коррупции и осознает их негативные последствия в социальных, экономических и других процессах общества		+
	УК-10-В-2 Соблюдает нормы права и морали, применяет правовые нормы и предусмотренные законом меры по противодействию коррупционному поведению и нейтрализации коррупционных проявлений		+
	УК-10-В-3 Идентифицирует угрозы и проявления экстремизма, терроризма, способен противодействовать им в профессиональной деятельности		+
общепрофессиональными компетенциями (ОПК):			
ОПК-1	**Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства**		**+**
	ОПК-1-В-1 Определяет актуальность и использует методы оценки значимости информации, информационных технологий и информационной безопасности в современном обществе, для обеспечения объективных потребностей личности, общества и государства		+
ОПК-2	**Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности**	**+**	**+**
	ОПК-2-В-1 Выбирает, обосновывает и применяет современные эффективные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе -	+	+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
	отечественного производства, для решения задач профессиональной деятельности		
ОПК-3	**Способен использовать необходимые математические методы для решения задач профессиональной деятельности**		+
	ОПК-3-В-1 Производит необходимые вычислительные работы с использование современных аппаратно-программных средств для решения задач профессиональной деятельности		+
ОПК-4	**Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности**	+	+
	ОПК-4-В-1 Разрабатывает и применяет при проектировании модели объектов защиты, нарушителя, угроз и систем защиты информации	+	+
ОПК-5	**Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности**	+	+
	ОПК-5-В-1 Использует нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере информационных технологий и телекоммуникаций	+	+
ОПК-6	**Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**	+	+
	ОПК-6-В-1 Организовывает и решает задачи защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций	+	+
ОПК-7	**Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности**	+	+
	ОПК-7-В-1 Разрабатывает оригинальные и применяет сертифицированные программные продукты для решения задач по эксплуатации систем защиты информации, а также задач проектно-технологического и организационно-управленческого типа	+	+
ОПК-8	**Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности**	+	+
	ОПК-8-В-1 Выполняет аналитический обзор, подбор, изучение и обобщение научно-технической литературы,	+	+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
	нормативных и методических документов в целях решения задач профессиональной деятельности		
ОПК-9	**Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности**	**+**	**+**
	ОПК-9-В-1 Производит выбор и обоснование средства криптографической и технической защиты информации для решения задач для решения задач проектно-технологического и организационно-управленческого типа	+	+
ОПК-10	**Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты**	**+**	**+**
	ОПК-10-В-1 Проводит экспертизу и разработку политики безопасности , организует и поддерживает выполнение комплекса мер по обеспечение информационной безопасности, управляет процессом их реализации в автоматизированных системах	+	+
ОПК-11	**Способен проводить эксперименты по заданной методике и обработку их результатов**	**+**	**+**
	ОПК-11-В-1 Планирует, проводит эксперименты и обрабатывает их результаты с использованием современных инструментальных средств	+	+
ОПК-12	**Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений**	**+**	**+**
	ОПК-12-В-1 Проводит предпроектное обследование объектов защиты, разрабатывает ТЭО и ТЗ в задачах модернизации и разработки систем защиты информации для АСУ	+	+
ОПК-13	**Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма**		**+**
	ОПК-13-В-1 Имеет собственную гражданскую, профессиональную и научную позицию в вопросах исторического развития России и развития патриотизма в профессиональной сфере		+
ОПК-4.1	**Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах**		**+**
	ОПК-4.1-В-1 Организует и проводит аудит, модернизацию, разработку и внедрение систем защиты информации		+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
ОПК-4.2	**Способен администрировать операционные системы, системы управления базами данных, вычислительные сети**		+
	ОПК-4.2-В-1 Осуществляет мониторинг, администрирование операционных систем, систем управления базами данных и вычислительных сетей		+
ОПК-4.3	**Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем**	+	+
	ОПК-4.3-В-1 Планирует порядок и осуществляет необходимые работы по установке, настройке , обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	+	+
ОПК-4.4	**Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем**	+	+
	ОПК-4.4-В-1 Применяет современные методы и средства диагностирования и мониторинга автоматизированных систем	+	+
профессиональными компетенциями (ПК):			
ПК*-1	**Способен диагностировать системы защиты автоматизированных систем**	+	+
	ПК*-1-В-1 Применяет современные методы и средства диагностирования автоматизированных систем	+	+
ПК*-2	**Способен администрировать системы защиты автоматизированных систем**	+	+
	ПК*-2-В-1 Решает задачи администрирования автоматизированных систем	+	+
ПК*-3	**Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций**	+	+
	ПК*-3-В-1 Оценивает характер и сложность нештатной ситуации, прогнозирует ее развитие и принимает адекватные меры по ее устранению	+	+
ПК*-4	**Способен осуществлять мониторинг защищенности информации в автоматизированных системах**	+	+
	ПК*-4-В-1 Выбирает оптимальные методы наблюдения, контроля и принятия решения по принятию мер обеспечения требуемой защищенности информации в автоматизированных системах	+	+
ПК*-5	**Способен проводить аудит защищенности информации в автоматизированных системах**	+	+
	ПК*-5-В-1 Выбирает и обосновывает рациональные методы и средства аудита защищенности информации	+	+

Код	Наименование компетенции/индикаторы	Вид государственного испытания, в ходе которого проверяется сформированность компетенции	
		государственный экзамен	защита ВКР
ПК*-6	**Способен устанавливать и настраивать средства защиты информации в автоматизированных системах**	+	+
	ПК*-6-В-1 Планирует порядок и осуществляет необходимые работы по установке и настройке аппаратно-программных средств защиты	+	+
ПК*-7	**Способен разрабатывать организационно-распорядительные документы в автоматизированных системах**	+	+
	ПК*-7-В-1 Опираясь на правовые нормы готовит организационно-распорядительные документы в автоматизированных системах	+	+
ПК*-8	**Способен проводить анализ уязвимостей внедряемой системы защиты информации**	+	+
	ПК*-8-В-1 Составляет отчеты по аудиту уязвимостей внедряемой системы защиты информации	+	+

Общая трудоемкость государственной итоговой аттестации составляет 6 зачетных единиц (216 академических часов).

2 Структура государственной итоговой аттестации

Государственная итоговая аттестация по направлению подготовки 10.03.01 Информационная безопасность включает:

- *подготовка к сдаче и сдача государственного экзамена;*
- *подготовка к процедуре защиты и защита выпускной квалификационной работы.*

3 Содержание государственного экзамена

3.1 Основные дисциплины образовательной программы и вопросы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускника и обеспечивают формирование соответствующих компетенций, проверяемых в процессе государственного экзамена

«Б1.Д.Б.6 Основы информационной безопасности»

соответствующие компетенции (для выбора основных дисциплин): ОПК-2, 6; УК-7

перечень вопросов и заданий:

1 Понятие информационной безопасности. Понятие национальной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства. Основные положения Стратегии национальной безопасности Российской Федерации.

2 Основные положения Доктрины информационной безопасности Российской Федерации. Интересы личности, общества и государства в информационной сфере.

3 Виды и свойства защищаемой информации.

4 Понятие угрозы безопасности информации. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.

5 Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы информационному обеспечению государственной политики Российской

Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

6 Угрозы безопасности информационных систем, как уже развернутых, так и создаваемых на территории России. Информационная система как объект защиты информации. Защита данных в вычислительных сетях.

7 Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.

8 Общая характеристика методов и средств защиты информации в автоматизированных системах (АС). Физические, программно-аппаратные, инженерно-технические, криптографические методы и средства обеспечения информационной безопасности АС.

9 Характеристика правовых и организационных методов обеспечения информационной безопасности.

10 Определение и назначение политики безопасности. Основные виды политики безопасности.

«Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности»
соответствующие компетенции (для выбора основных дисциплин): ОПК-5-6, 10
перечень вопросов и заданий:

1. Информация как объект правового регулирования, виды информации, защищаемой законодательством Российской Федерации. Основные нормативно-правовые документы, регламентирующие деятельность по защите информации.

2. Коммерческая тайна, определение понятия в соответствии с нормативным документом. Организация режима коммерческой тайны на предприятии. Перечень сведений, которые нельзя относить к коммерческой тайне.

3. Лицензирование в области защиты информации. Перечень видов деятельности по защите информации. Требования нормативных документов ФСТЭК и ФСБ к составу пакета документов для оформления лицензии.

4. Определение понятия «сертификация». Цели системы сертификации средств защиты информации по требованиям безопасности информации. Функции ФСТЭК и ФСБ в области сертификации средств защиты информации.

5. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Структура сил и средств организационной защиты информации.

6. Функции, задачи и структура службы безопасности организации. Принципы организации службы безопасности организации. Основные документы, регламентирующие деятельность службы безопасности объекта.

7. Защита государственной тайны. Регуляторы в области защиты государственной тайны. Требования нормативных документов по защите государственной тайны.

8. Основные положения допуска персонала предприятия к конфиденциальной информации. Основные положения допуска должностных лиц и граждан к государственной тайне. Формы допуска. Нормативные документы, регламентирующие порядок оформления допуска к государственной тайне.

9. Политика информационной безопасности. Основные требования нормативных документов при разработке политики безопасности предприятия, структура и состав документа.

10. Практическое задание. Определить вид тайны в документах предприятия и указать перечень федеральных нормативных документов и организационно-распорядительной документации предприятия по защите этой информации. Заполнить таблицу.

Таблица

Наименование документа или сведений	Вид тайны	Перечень федеральных и локальных нормативных документов по защите информации
Трудовой договор с сотрудником		
Технологическая карта изделия		
Конструкторская документация		
Сведения о научной деятельности в оборонной промышленности		
Медицинская карта пациента		
Реквизиты банковской карты		
Сведения о радиационной обстановке на предприятии		

«Б1.Д.Б.10 Программно-аппаратные средства защиты информации»

соответствующие компетенции (для выбора основных дисциплин): ОПК-4.3, 10; УК-1

перечень вопросов и заданий:

1. Аутентификация, авторизация и администрирование действий пользователя. Основные факторы аутентификации. Двухфакторная аутентификация.
2. Средства защиты информации от НСД. Основные функции СЗИ от НСД: доверенная загрузка, изолированная программная среда, мандатная модель разграничения доступа, аппаратная аутентификация, контроль целостности программно-аппаратных средств ПК.
3. Электронно-цифровая подпись и функция хэширования. Схема формирования электронной подписи. Усиленная квалифицированная подпись. Усовершенствованная электронная подпись. Структура цифрового сертификата стандарта X.509.
4. Функции межсетевых экранов. Фильтрация. Выполнение функций посредничества. Дополнительные возможности межсетевых экранов.
5. Концепция построения виртуальных защищенных сетей. Основные понятия и функции сети VPN. Варианты построения виртуальных защищенных каналов.
6. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ. Методы защиты от вредоносного ПО.
7. Аппаратные носители ключевой информации. Классификация носители ключевой информации. Общая структура USB-токена. Дополнительные возможности USB-токенов: шифрование, формирование электронной подписи, защищенная FLASH-память, хранение и проверка цифрового отпечатка.
8. Система разграничения доступа. Общая структура системы разграничения доступа. Модели разграничения доступа: дискреционная, мандатная и ролевая. Достоинства и недостатки моделей разграничения доступа. Особенности системы разграничения доступа ОС Windows.
9. Аппаратные и программно-аппаратные средства криптозащиты данных. Основные элементы аппаратно-программной системы криптографической защиты данных серии «Криптон».
10. Определите методы и средства аутентификации для трех типов учетной записи автоматизированной системы:

- пользователь рабочей станции;
- бухгалтер организации, использующий систему дистанционного банковского обслуживания;
- системный администратор.

Обоснуйте выбор. Определите основные моменты политики идентификации и аутентификации для данных учетных записей АС.

«Б1.Д.Б.17 Дискретная математика»

соответствующие компетенции (для выбора основных дисциплин): ОПК-1, 5, 7-8; УК-1-2

перечень вопросов и заданий:

1. Понятие множества. Операции над множествами. Диаграммы Эйлера-Венна.
2. Мощность множества. Счетные множества.
3. Прямое произведение множеств. Понятие n-местного отношения.

4. Соответствия между множествами. Функции. Инъекция, сюръекция, биекция.
5. Отношения. Бинарные отношения. Свойства отношений.
6. Булевы функции одной и двух переменных.
7. Булевы функции. Способы задания. Существенные и фиктивные переменные.
8. Схемы из функциональных элементов.
9. Понятие рекуррентного соотношения. Линейные рекуррентные соотношения. Метод решения.
10. Графы. Основные понятия и определения. Изоморфизм графов.

«Б1.Д.Б.19 Методы и средства криптографической защиты информации»

соответствующие компетенции (для выбора основных дисциплин): ОПК-2, 4.3, 9; УК-1

перечень вопросов и заданий:

1. Шифры: перестановки, замены, многоалфавитной подстановки, шифр Вернама, Вижинера, гаммирование.

2. Надежность криптосистем. Элементы криптоанализа. Виды атак. Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость

3 Современные симметричные криптосистемы: блочные шифры DES, режимы работы DES, ГОСТ, их характеристики достоинства и недостатки.

4. Криптографические протоколы. Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей

5. Электронная цифровая подпись: понятие Хэш-функции. Алгоритмы ЭЦП: RSA, Эль Гамаля.

Практические задания

1. Условие задачи:

Абоненты некоторой сети используют ассиметричную криптосистему RSA для безопасной передачи сообщений. Отправителю необходимо передать сообщение M = 2, используя следующие параметры P=11, Q=17, Открытый ключ ko = 7. Для указанных параметров необходимо сформировать криптограмму (шифротекст) для передачи получателю. Получатель должен расшифровать полученное сообщение.

Задание:

1. Представить обобщенную схему асимметричной криптосистемы RSA.
2. Найти секретный ключ получателя.
3. Рассчитать криптограмму (шифротекст).
4. Расшифровать полученную криптограмму.
5. Сделать выводы.

2. Условие задачи:

Абоненты некоторой сети используют ассиметричную криптосистему RSA для безопасной передачи сообщений. Отправителю необходимо передать сообщение M = 4, используя следующие параметры P=29, Q=31, Открытый ключ ko = 11. Для указанных параметров необходимо сформировать криптограмму (шифротекст) для передачи получателю. Получатель должен расшифровать полученное сообщение.

Задание:

1. Представить обобщенную схему асимметричной криптосистемы RSA.
2. Найти секретный ключ получателя.
3. Рассчитать криптограмму (шифротекст).
4. Расшифровать полученную криптограмму.
5. Сделать выводы.

3. Условие задачи:

Два абонента сети используют незащищенный от прослушивания канал связи. Двум абонентам сети известны открытые параметры: два числа P = 97, g = 5 и у каждого свои секретные параметры: два числа KA = 23, KB = 29. Используя протокол распределения ключей Диффи-Хеллмана, необходимо найти общий секретный ключ K, который они будут использовать для шифрования и дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Задание:

1. Представить обобщенную схему прямого обмена ключами по протоколу Диффи-Хэллмана.
2. Рассчитать открытые ключи абонентов сети.

3. Вычислить общий секретный ключ на каждой стороне.
4. Сделать выводы.

4. Условие задачи:

Два абонента сети используют незащищенный от прослушивания канал связи. Двум абонентам сети известны открытые параметры: два числа P = 71, g = 7 и у каждого свои секретные параметры: два числа KA = 19, KB = 31. Используя протокол распределения ключей Диффи-Хеллмана, необходимо найти общий секретный ключ K, который они будут использовать для шифрования и дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Задание:

1. Представить обобщенную схему прямого обмена ключами по протоколу Диффи-Хэллмана.
2. Рассчитать открытые ключи абонентов сети.
3. Вычислить общий секретный ключ на каждой стороне.
4. Сделать выводы.

5. Условие задачи:

Абоненты некоторой сети применяют электронную подпись методом RSA с общими параметрами N = 65, Открытый ключ ko = 5. Для указанных параметров необходимо проверить подлинность подписанных сообщений: Хэш-функция передаваемого сообщения m = H(M) = 10, электронная подпись S=30.

Задание:

1. Представить обобщенную схему электронной подписи RSA.
2. Найти секретный ключ отправителя.
3. Рассчитать электронную подпись.
4. Получить исходное сообщение (хэш-функцию).
5. Сделать выводы о подлинности подписанных сообщений.

«Б1.Д.Б.20 Техническая защита информации»

соответствующие компетенции (для выбора основных дисциплин): ОПК-10-11

перечень вопросов и заданий:

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации.
2. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
3. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации.
4. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.
5. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации. Средства акустической разведки. Дальность перехвата речевого сигнала средством акустической разведки направленными микрофонами.
6. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой основными техническими средствами и системами (ОТСС).
7. Экранирующие материалы, их основные характеристики. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).
8. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Средства звукоизоляции и виброизоляции выделенных помещений. Звукоизолирующие кабины. Специальные защищенные помещения.
9. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.
10. Обнаружить закладное устройство (имитатор сигналов «Шиповник 2») с использованием детектора поля DP-20.

«Б1.Д.Б.26 Аппаратные средства вычислительной техники»

соответствующие компетенции (для выбора основных дисциплин): ОПК-2, 4.4; УК-1

перечень вопросов и заданий:

1. Структура ЭВМ и назначение ее элементов. ОЗУ, ПЗУ, контроллер внешнего устройства.
2. Общая структура центрального процессора. Операционное и управляющие устройства.
3. Принцип магистральной организации ЭВМ. Системная шина: шина адреса, управления и данных.
4. Элементы памяти, их назначение, возможности и принцип работы. Динамическая и статическая память.
5. Многоуровневая организация структуры памяти ЭВМ. Основные требования к памяти: объем, быстродействие, стоимость и энергонезависимость.
6. Организация ввода\вывода в ЭВМ. Программно-управляемая передача данных: синхронная и асинхронная.
7. Система команд МП. Основные группы команд. Машинный формат команды.
8. Системы ввода-вывода. Способы организации обмена данными МП с внешними устройствами. Понятие порта.
9. Сегментная организация памяти. Логический и физический адрес.
10. Вычислительные системы в системах управления. Микроконтроллеры.

«Б1.Д.Б.30 Защита информационных процессов в автоматизированных системах»

соответствующие компетенции (для выбора основных дисциплин): ОПК-4.3, 10; УК-1

перечень вопросов и заданий:

1. Основные угрозы безопасности информации в автоматизированных системах (АС), специфика возникновения угроз в открытых сетях, особенности защиты информации на узлах компьютерной сети АС.
2. Система лицензирования и сертификации средств защиты информационных процессов. Аттестация защищенных систем. Структуры в РФ, обеспечивающие лицензирование и сертификацию.
3. Нормативно-правовая база в области защиты информационных процессов в автоматизированных системах.
4. Основные положения ГОСТ Р 51583-2000 Порядок создания автоматизированных систем в защищенном исполнении.
5. Требования к подсистемам аудита информационных процессов. Подсистемы подтверждения подлинности отправки и получения сообщения.
6. Понятие уязвимости АС. Основные уязвимости в АС. Средства анализа уязвимостей.
7. Гарантии безопасности информационных процессов в автоматизированных системах. Уровни гарантий. Методология анализа гарантий.
8. Понятие риска в автоматизированных системах и порядок его оценки.
9. Назначение, особенности установки и применения сетевых средств для защиты информационных процессов в автоматизированных системах.
10. Характеристика программно-аппаратных средств защиты информационных процессов в автоматизированных системах.

«Б1.Д.Б.31 Теория информационной безопасности и методология защиты информации»

соответствующие компетенции (для выбора основных дисциплин): ОПК-4-5; УК-1

перечень вопросов и заданий:

1. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
2. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация и характеристика угроз в КС
3. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Основные принципы построения политики безопасности.
4. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели.
5. Классификация и общая характеристика средств и методов защиты информации в КС.
6. Классификация и характеристика формальных моделей систем защиты информации.

7. Характеристика целевых функций и критериев оценки качества, используемых при создании систем защиты информации. Привести примеры критериев экономического, технического и социального вида для оценки качества проектируемой системы.

8. Характеристика моделей и методов оценки уровня защищенности автоматизированных систем

9. Основные понятия и принципы риск-анализа в исследованиях систем защиты информации.

10. Построить табличную модель исходов теории игр в задаче принятия решений.

«Б1.Д.Б.32 Экономика защиты информации»

соответствующие компетенции (для выбора основных дисциплин): ОПК-12

перечень вопросов и заданий:

1. Экономика защиты информации как наука, задачи экономики защиты информации.
2. Экономические проблемы информационных ресурсов и защиты информации.
3. Особенности ценообразования на информационные продукты.
4. Характеристика основных методов определения затрат на обеспечение безопасности информации.
5. Экономическая оценка объектов интеллектуальной собственности.
6. Анализ, оценка и способы минимизации предпринимательских рисков.
7. Экономический эффект и экономическая эффективность защиты информации.
8. Инвестиции в объекты защиты информации: понятие, виды, задачи.
9. Планирование затрат на информационную безопасность.
10. Оценка эффективности инвестиций в защиту информации.

«Б1.Д.Б.35 Безопасность информационных систем и баз данных»

соответствующие компетенции (для выбора основных дисциплин): УК-1

перечень вопросов и заданий:

1. Автоматизированные информационные системы: понятие, основные определения. База данных: понятие, уровни представления базы данных. Система управления базами данных: понятие, архитектура, функции. Роль и состав информационного обеспечения АИС. Угрозы на информационные системы.

2. Целостность данных. Транзакция: понятие, свойства транзакций. Функция восстановления баз данных.

3 Методы и средства защиты данных в СУБД от сбоев и несанкционированного доступа. Методы управления доступом в современных базах данных.

4. Проектирование баз данных (инфологическое, даталогическое, физическое). Модель "Сущность-Связь". Правила перехода от инфологической к даталогической модели данных. Нормализация схем отношений.

5 Основные понятия и определения реляционной модели данных. Свойства отношений. Структурированный язык запросов.

Практические задания

1. Проектируется база данных для банка, содержащая информацию о клиентах и их счетах. Информация о клиенте содержит: имя, адрес, телефон и номер страхового полиса. Счета имеют номера, типы (сберегательный, чековый и т.п.) и балансы. Необходимо также записывать клиентов, являющихся владельцами счетов. Построить ER-диаграмму предметной области, дать формализованное описание, учитывая следующие ограничения:

- только один клиент может быть указан как владелец счета;
- один клиент не может иметь более одного счета;
- каждый адрес имеет три компонента: улица, город и страна. Клиенты могут иметь любое число адресов и телефонов.

2. В базе данных отдела кадров хранятся сведения о сотрудниках организации в отношении Сотрудник (Табельный номер, Фамилия, Имя, Отчество, Номер кабинета, Количество детей) и сведения о телефонах Телефон (Номер кабинета, Номер телефона) (примечание: в каждом кабинете может быть не более одного номера телефона). Отношения Сотрудник и Телефон связаны по внешнему ключу Номер кабинета. Используя команду Select языка SQL, запишите следующие запросы:

- найти среднее количество детей сотрудников;
- вывести в алфавитном порядке ФИО сотрудников первого кабинета;
- определить номер телефона для сотрудника Иванова Ивана Ивановича;
- вывести ФИО сотрудников, у которых номер телефона 41-41-41.

3. База данных видеофильмов содержит следующие отношения Фильм (Название фильма, Год выпуска, Код жанра, Код режиссера, Описание, Длительность), Жанр (Код жанра, Название жанра), Режиссер (Код режиссера, Фамилия, Имя, Отчество). С помощью команд языка SQL выполните следующие действия:

- ввести в БД информацию о фильме "Иван Васильевич меняет профессию", год выпуска 1973, жанр – комедия, режиссер –Л. И. Гайдай, длительность – 90 минут;
- удалить из БД все фильмы, выпущенные до 1970 года;
- в БД фильм "Три плюс два" был неверно причислен к жанру трагедия. Изменить значение этого свойства на жанр комедия, узнав код жанра из отношения Жанр;

Используя команду Select языка SQL, запишите следующие запросы:

- вывести в алфавитном порядке ФИО режиссеров, снявших более 10 фильмов.
- вывести в алфавитном порядке список фильмов режиссера Никиты Сергеевича Михалкова;
- подсчитать количество фильмов, выпущенных в 2023 году;

4. В базе данных отдела кадров хранятся сведения о сотрудниках организации в отношении Сотрудник (Табельный номер, Фамилия, Имя, Отчество, Номер кабинета, Количество детей) и сведения о телефонах Телефон (Номер кабинета, Номер телефона) (примечание: в каждом кабинете может быть не более одного номера телефона). Отношения Сотрудник и Телефон связаны по внешнему ключу Номер кабинета. Используя команду Select языка SQL, запишите следующие запросы:

- найти среднее количество детей сотрудников;
- вывести в алфавитном порядке ФИО сотрудников первого кабинета;
- определить номер телефона для сотрудника Иванова Ивана Ивановича;
- вывести ФИО сотрудников, у которых номер телефона 41-41-41.

5. В базе данных отдела кадров хранятся сведения о сотрудниках организации в отношении Сотрудник(Табельный номер, Фамилия, Имя, Отчество, Номер кабинета, Количество детей) и сведения о телефонах Телефон(Номер кабинета, Номер телефона). Предположим, в системе зарегистрированы пользователи User1, User2 и User 3. С помощью команд языка SQL

а) создать пользователя User3 и назначить ему следующие права:

-чтение, запись, редактирование, удаление та таблицу Сотрудник;

-чтение на таблицу Телефон;

-включить возможность делегирования прав другим пользователям;

в) пользователю User3 назначить все права на таблицу Телефон (без возможности их дальнейшей передачи).

«Б1.Д.В.9 Защита доступа в автоматизированных системах»

соответствующие компетенции (для выбора основных дисциплин): УК-1; ПК-4-6*

перечень вопросов и заданий:

1. Методы защиты от несанкционированного доступа.
2. Средства защиты от несанкционированного доступа.
3. Основные характеристики технических средств защиты от НСД.
4. Организация работ по защите от НСД
5. Требования по защите информации от НСД для АС
6. Принципы настройки межсетевых экранов.
7. Примеры атак, предотвращаемых межсетевыми экранами. Атаки на сетевые экраны.
8. Понятие Intrusion Detection Systems (IDS). Причины использования IDS. Классификация IDS.
9. Организация безопасного доступа к Интернет сотрудников компании.
10. Защита от случайных или преднамеренных утечек конфиденциальной информации.

«Б1.Д.В.10 Организация работ по защите персональных данных»

соответствующие компетенции (для выбора основных дисциплин): УК-1; ПК-1-2, 5, 7*

перечень вопросов и заданий:

1. Характеристика категорий персональных данных в соответствии с нормативными документами. Безопасность персональных данных, принципы обработки персональных данных.

2. Информационная система персональных данных, пояснить состав и назначение на основании нормативного документа. Уровень защищенности информационной системы персональных данных, факторы, определяющие уровень защищенности.

3. Основные показатели уровня исходной защищенности информационной системы персональных данных. Требования нормативных документов к содержанию мер по защите информационных систем персональных данных.

4. Модель угроз безопасности информационных систем персональных данных. Основы построения модели угроз.

5. Характеристики нарушителей безопасности персональных данных, описание категорий.

6. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в соответствии с нормативными документами Роскомнадзора.

7. Поэтапный порядок организации обработки персональных данных на предприятии. Требования к локальным организационно-распорядительным документам оператора по защите персональных данных.

8. Характеристика комплекса мер и средств для организации защиты персональных данных на предприятии.

9. Виды и мероприятия по аудиту системы защиты персональных данных. Основные нарушения в ходе проверок сайтов организаций.

10. Ответственность оператора за нарушения требований по защите персональных данных. Привести нормативные документы.

11. Практическое задание. Что считать трансграничной передачей персональных данных (ТГП)? Привести названия нормативных документов.

— В каком случае трансграничная передача может быть включена в согласие по обработке персональных данных?

— Если филиал российской компании на территории иностранного государства не считается самостоятельным юридическим лицом по законодательству иностранного государства, обмен персональными данными с этим филиалом будет считаться ТГП?

— Считается ТГП использование Google Analytics в адрес Google?

— Будет считаться ТГП передача только телефонных номеров без дополнительной информации.

— Считается ТГП передача адресов электронной почты?

6. Будет считаться ТГП ситуация, когда у иностранного юридического лица есть работники – граждане РФ, но работают они за рубежом?

«Б1.Д.В.Э.6.1 Информационная безопасность в сетях и телекоммуникациях»

соответствующие компетенции (для выбора основных дисциплин): УК-1; ПК-1-2, 8*

перечень вопросов и заданий:

1. Современные угрозы сетевой безопасности. Инструменты злоумышленника. Распространенные сетевые атаки.

2. Обеспечение безопасности сетевых устройств. Защита доступа к сетевым устройствам. Мониторинг сетевых устройств и управление ими.

3. Аутентификация, авторизация и учет (AAA). Назначение AAA. Локальная аутентификация AAA. Серверное решение AAA.

4. Внедрение технологий межсетевого экрана. Зональные межсетевые экраны. Списки контроля доступа.

5. Технологии системы предотвращения вторжений IPS. Сигнатуры IPS. Внедрение IPS.

6. Обеспечение безопасности локальной сети. Безопасность оконечных устройств. Факторы, которые необходимо учитывать при обеспечении безопасности на канальном уровне.

7. Виртуальные частные сети VPN. Компоненты сети IPSec VPN и их функционирование.

8. Управление безопасной сетью. Тестирование безопасности сети. Разработка комплексной политики безопасности.

9. Методы тестирования сети на проникновение. Этапы тестирования сети на проникновение. Сканирование сети, портов, уязвимостей. Определение активных сервисов в сети.

10. Уязвимости: понятие, номенклатура, типы. Поиск и эксплуатация уязвимостей. Парольные атаки на различные сервисы. Использование фреймворка Metasploit для поиска и эксплуатации уязвимостей.

«Б1.Д.В.Э.7.1 Обработка экспериментальных данных на электронно-вычислительных машинах»

соответствующие компетенции (для выбора основных дисциплин): УК-1; ПК-2-3*

перечень вопросов и заданий:

1. Основные цели обработки экспериментальных данных.
2. Источники и вид представления экспериментальных данных.
3. Эмпирическая функция распределения.
4. Оценки параметров распределения и их свойства.
5. Графический и аналитические методы обработки результатов.
6. Математические и статистические системы, которые можно использовать для обработки экспериментальных данных.
7. Показатели асимметрии и эксцесса.
8. Статистическая гипотеза.
9. Теория погрешностей. Погрешности прямых измерений, случайные, приборные погрешности.
10. Составьте произвольный статистический ряд. Постройте и рассчитайте эмпирическую функцию распределения и плотности.

3.2 Порядок проведения государственного экзамена и методические материалы, определяющие процедуру оценивания результатов освоения образовательной программы на этом этапе государственных испытаний

Экзаменационные билеты междисциплинарного экзамена (государственного экзамена) разрабатываются выпускающей кафедрой на основе утвержденной Ученым Советом факультета программы и утверждаются председателем соответствующей экзаменационной комиссии.

Экзаменационные билеты состоят из двух теоретических вопросов и одной задачи. Экзамен проводится в устой и письменной форме: ответы на теоретические вопросы приводятся в устной форме, результаты решения задач, а также схемно-технические пояснения к устным вопросам приводятся в письменном виде на специально выданных (проштампованных) выпускникам листах бумаги.

Время, отводимое на подготовку, не превышает 3 часов.

В процессе выполнения творческого задания экзаменуемый может пользоваться справочной, учебной и научной литературой, список которой оговорен настоящей программой.

Результаты государственного экзамена определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно". Оценки "отлично", "хорошо", "удовлетворительно" означают успешное прохождение государственного аттестационного испытания.

При определении оценки знаний и умений, выявленных при сдаче государственного экзамена, принимаются во внимание уровень теоретической и практической подготовки выпускника.

Оценка "отлично" выставляется тому, кто глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязать теорию с практикой, свободно справился с поставленной задачей при выполнении мини-проекта, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении задания, правильно обосновывает принятие решения, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка "хорошо"– тому, кто твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач при выполнении мини-проекта, владеет необходимыми навыками и приемами их выполнения, однако не смог всесторонне проанализировать весь теоретический и практический материал по мини-проекту. При ответах на

экзаменационные билеты допускал неточности в основной сущности вопроса и его практического применения.

Оценка "удовлетворительно" выставляется тому, кто имеет знания только основного материала, но не усвоил его деталей, тема мини-проекта в целом раскрыта, однако анализ теоретических и практических положений проведен неглубоко, допускает неточности, недостаточные правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения в выполнении практических работ, при ответах на вопросы экзаменуемый затруднялся отвечать на некоторые вопросы.

Оценка "неудовлетворительно" выставляется тому, кто не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, в мини-проекте допущены существенные ошибки или последний выполнен не по заданию.

3.3 Перечень рекомендуемой литературы для подготовки к государственному экзамену

1. Алферов, А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005. – 480 с.
2. Аралбаев, Т.З. Проектирование вычислительных систем [Электронный ресурс]/Аралбаев Т.З., Галимов Р.Р., Хасанов Р.И.-ОГУ, 2012.
3. Болодурина, И.П. Проектирование компонентов распределенных информационных систем: учебное пособие [Электронный ресурс]/Болодурина И.П., Волкова Т.В.-ОГУ, 2012.
4. Гражданский кодекс Российской Федерации [Текст].-Москва: Проспект КноРус,2014.-608 с.
5. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов / В. Г. Грибунин, В. В. Чудовский . - М.: Академия, 2009. - 413 с. - (Высшее профессиональное образование). - Библиогр.: с. 403-406.
6. Девянин, П.Н. Модели безопасности компьютерных систем [Текст] : учеб.пособие для вузов / П.Н. Девянин. - М. : Академия, 2005. - 144 с.
7. Доктрина информационной безопасности Российской Федерации" (утв. Президентом РФ 09.09.2000 N Пр-1895).
8. Федеральный закон «Об информации, информационных технологиях и о защите информации»от 27.07.2006 N 149-ФЗ (последняя редакция).
9. Федеральный закон РФ "О персональных данных" (152-ФЗ) 2017.
10. Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне" (в редакции, актуальной с 15 сентября 2015 г.,
11. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
12. Заботина, Н.Н.Проектирование информационных систем [Текст]:учебное пособие для студентов высших учебных заведений/ Н.Н. Заботина.-Москва: ИНФРА-М, 2013.-331 с.
13. Казанцев, С.Я., Згадзай О.Э., Оболенский Р.М. и др. Правовое обеспечение информационной безопасности: Учебное пособие для студентов васш. учеб.заведений. – М.: Издательский центр «Академия», 2007. – 240 с.
14. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов / А. А. Малюк . - М. : Горячая линия-Телеком, 2004. - 280 с.
15. Организационно-правовое обеспечение информационной безопасности [Текст] : учеб.пособие для студентов вузов, обучающихся по специальностям 090102 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммукационных систем" / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с.
16. Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] : учеб. пособие / С. Н. Семкин [и др.] . - М. : Гелиос АРВ, 2005. - 192 с.
17. Семененко,В.А. Программно-аппаратная защита информации [Текст] : учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров . - М. : МГИУ, 2007. - 340 с. - Библиогр.: с. 290-295. - Прил.: с. 296-339. - ISBN 978-5-2760-1169-1.

18. Торокин, А. А. Инженерно-техническая защита информации [Текст] : учебное пособие для вузов / А. А. Торокин . - М. : Гелиос АРВ, 2005. - 960 с. : ил.. - Библиогр.: с. 934-949.
19. Хохлов, Г. И. Основы теории информации: учеб. пособие / Г. И. Хохлов . - М. : Академия, 2008. - 172 с.

3.4 Интернет-ресурсы

1. Anti-Malware | https://www.anti-malware.ru/
2. Geektimes | https://geektimes.ru/hub/infosecurity/
3. ISO27000.RU http://www.iso27000.ru/
4. Security Lab | http://www.securitylab.ru/
5. Threatpost https://threatpos
6. Ассоциация по вопросам защиты информации BISA http://bis-expert.ru/
7. Журнал “Information Security” http://www.itsec.ru/articles2/allpubliks
8. Клуб информационной безопасности http://wiki.informationsecurity.club/doku.php/main
9. Научный журнал «Вопросы кибербезопасности» http://cyberrus.com/
10. Официальный сайт ФСТЭК РОССИИ fstec.ru

4 Выпускная квалификационная работа

4.1 Структура выпускной квалификационной работы и требования к ее содержанию и оформлению

Государственная итоговая аттестация включает защиту выпускной квалификационной работы (ВКР).

Целью выпускной квалификационной работы является достижение выпускником необходимого уровня знаний, компетенций, умений и навыков, позволяющих ему как будущему специалисту по информационной безопасности успешно воздействовать на объекты управленческой деятельности и добиваться высоких технико-экономических показателей их развития в долгосрочной перспективе. Сопутствующими целями ВКР являются:

- подготовка конкретного плана мероприятий по совершенствованию деятельности объекта исследования;
- овладение теоретическими знаниями и практическими навыками для подготовки, принятия и реализации эффективных решений;
- проведение системных исследований объекта защиты и практической реализации полученных знаний.

Для достижения поставленных целей магистрант должен решить следующие задачи:

- обосновать актуальность выбранной темы ВКР, сформулировать цель и задачи исследований;
- проанализировать теоретические и методические положения, нормативно-техническую документацию, справочную и патентную литературу, документы ФСТЭК, законодательные акты в соответствии с выбранной темой ВКР;
- обосновать научную новизну ВКР;
- решить проблемы развития системы защиты информации как объекта исследования;
- обосновать экономическую эффективность разработанных мероприятий.

ВКР является самостоятельным научным исследованием, выполняемым под руководством научного руководителя (при необходимости, с привлечением одного или двух научных консультантов).

Первый раздел ВКР посвящен системному анализу задач ВКР, включающему в себя: объект, предмет, границы исследований, цель; описание предмета исследований, проблемы практики, проблемы теории, основное противоречие, цель исследования, задачи для достижения цели и гипотеза их решения; библиография (базовая, патентная и периодическая), одной из основных задач раздела является построение моделей нарушителя и угроз для защищаемого объекта;.

Второй раздел содержит теоретическую часть: разработку моделей, алгоритмов и методов защиты, в частности, моделей системы защиты и алгоритмов обеспечения их безопасности.

Третий раздел посвящен вопросам разработки системы защиты объекта или отдельных подсистем и ее элементов: разработке структуры и архитектуры, выбору и обоснованию инструментария разработки, проектированию структуры данных, вопросам интеграции с аналитическим приложением, отладке и квалификационному тестированию, регистрации базы данных и разработанных программ.

Четвертый раздел включает: экспериментальную оценку эффективности внедрения результатов исследования и разработки, разработку методики оценки эффективности, оценка результатов, рекомендации по использованию результатов ВКР и направления дальнейших исследований.

Структура каждой ВКР утверждается научным руководителем работы, но при необходимости, согласовывается с председателем методической комиссии по направлению 10.03.01 – Информационная безопасность.

Устанавливаются стандартные для научных работ требования к содержанию ВКР:

- стиль изложения ВКР – научно-технический, не допускается использование разговорных оборотов и непринятых терминов;

- текст, таблицы и иллюстрации выполняются согласно действующему стандарту организации для выпускных квалификационных студенческих работ.

Защита ВКР осуществляется в виде публичного выступления с представлением графического материала или презентации. По окончании защиты пояснительная записка - ВКР и графический материал в виде стандартных форматов - сдается в архив. Пояснительная записка должна содержать результаты по всем разделам ВКР. Объем пояснительной записки ВКР – не менее 60 страниц; графический материал должен отражать постановку всех задач ВКР и результаты их решения.

Государственная аттестационная комиссия для приема защиты ВКР назначается в количестве не менее пяти членов, трое из которых являются представителями работодателей.

Председателем комиссии назначается сторонний специалист.

Государственная аттестационная комиссия по итогам защиты ВКР и может делать заключение о целесообразности обучения бакалавра в магистратуре.

4.2 Порядок выполнения выпускной квалификационной работы

Текстовая часть ВКР содержит следующие структурные элементы:

– титульный лист;
– задание на ВКР;
– аннотация (на русском и иностранном языках);
– содержание;
– введение;
– основную часть;
– заключение;
– список использованных источников;
– перечень условных обозначений (при необходимости);
– приложения (при необходимости).

В ВКР вкладываются заполненные и подписанные бланки: «Лист нормоконтроля ВКР», «Отзыв руководителя о ВКР», справка о степени оригинальности содержания ВКР.

Титульный лист пояснительной записки оформляется в соответствии с требованиями СТО 02069024.101-2015.

Научными направлениями кафедры являются:

- разработка имитационных моделей, методов и средств мониторинга состояния защищенности распределенных информационно-вычислительных систем и мобильных объектов информатизации

- защита информации в распределенных информационно-вычислительных системах и телекоммуникациях.

Тематика ВКР определяется потребностями экономики региона и научными направлениями кафедры. Темы и руководители ВКР утверждаются на заседании кафедры в начале первого семестра обучения.

Тематика ВКР включает в себя решение следующих задач:

- разработка и исследование методов и средств повышения уровня защищенности технико- современных РИВС для предприятий и организаций Оренбургской области;

- исследование технико-экономической эффективности базовых систем информационной безопасности РИВС и поиск путей их совершенствования;

- исследование уровня информационной защищенности РИВС и разработка методов и средств снижения риска от несанкционированного доступа к информации;

- разработка и исследование новых информационных технологий систем информационной безопасности РИВС;

- разработка и исследование методов защитного мониторинга распределенных систем транспортировки нефте-газопродуктов;

- разработка и исследование распределенных систем защиты информации на основе современных Интернет-технологий и спутниковых навигационных средств;

- исследование и разработка мобильных систем защитного мониторинга сложных распределенных промышленных объектов нефте-газодобычи на основе геоинформационных технологий;

- разработка и исследование распределенных систем дистанционного обучения студентов-безопасников;

- разработка математических и имитационных моделей для поиска закономерностей возникновения и нейтрализации сетевых аномалий в РИВС.

4.3 Порядок защиты выпускной квалификационной работы

Защита ВКР происходит публично. Она носит характер дискуссии и происходит в обстановке высокой требовательности и принципиальности; обстоятельному анализу должны подвергаться достоверность и обоснованность всех выводов и рекомендаций, содержащихся в работе. Кроме членов экзаменационной комиссии на защите желательно присутствие научного руководителя работы, а также возможно присутствие других студентов, преподавателей и администрации.

Заседание Государственной экзаменационной комиссии начинается с того, что секретарь объявляет о защите, указывая ее название, фамилию, имя, отчество ее автора, а также докладывает о наличии необходимых в деле документов, передает председателю расчетно-пояснительную записку и все необходимые материалы, после чего выпускник получает слово для доклада.

В своем выступлении на заседании ГЭК выпускник должен отразить:

- актуальность темы;
- цель и задачи ВКР;
- теоретические и методические положения, на которых базируется ВКР;
- результаты проведенного анализа изучаемого явления;
- конкретные предложения по решению проблемы или совершенствованию соответствующих моделей, процессов и т.п. с обоснованием возможности их реализации в условиях конкретного предприятия; экономический, социальный и экологический эффекты от разработок.

В докладе следует выделять главные вопросы без детализации частностей. Особое внимание необходимо сосредоточить на собственных разработках.

Время выступления студента не должно превышать 10 минут.

После окончания доклада члены ГЭК задают вопросы, которые секретарь записывает вместе с ответами в протокол. Члены Государственной экзаменационной комиссии и лица, приглашенные на защиту, в устной форме могут задавать любые вопросы по проблемам, затронутым в работе, методам исследования, уточнять результаты и процедуру экспериментальной работы и т.п. Отвечая на вопросы, нужно касаться только существа дела. Затем секретарь зачитывает отзыв руководителя и рецензию на ВКР, и выпускник отвечает на замечания рецензента. Общая продолжительность защиты не должна превышать 20 минут.

4.4 Критерии оценивания выпускной квалификационной работы

Результаты защиты ВКР определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно". Оценки "отлично", "хорошо", "удовлетворительно" означают успешное прохождение государственного аттестационного испытания.

Оценки выставляются на основе выполнения и защиты ВКР и соответствия уровню подготовки выпускника требованиям ФГОС ВО.

При оценке ВКР принимаются во внимание уровень теоретической, научной и практической подготовки выпускников, их профессиональной подготовленности в соответствии с требованиями ФГОС ВО, установленные как на основе анализа качества выполненной ВКР, так и во время ее защиты. Оцениваются: актуальность и важность темы для науки и практики; выполнения по заказу предприятия; наличие публикаций по защищаемой теме; проведение экспериментальных, лабораторных и производственных испытаний.

Оценка ВКР обучающихся производится по следующим критериям:

- оценка «отлично» выставляется обучающемуся, если показал большой объем выполненных работ; типовыми примерами таких работ являются - натурные испытания или вычислительный эксперимент; многовариантный анализ технологического процесса; интересные решения в специальной части ВКР, а также доказал своими ответами на вопросы комиссии, что он глубоко и прочно усвоил ООП; исчерпывающе, последовательно, четко и логически стройно излагает материал, умеет тесно увязывать теорию с практикой; не затрудняется с ответами на проблемно-ориентированные вопросы; правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения инженерных задач;

- оценка «хорошо» выставляется обучающемуся, если показал необходимый объем выполненных работ, а также доказал своими ответами на вопросы комиссии, что он глубоко и прочно усвоил ООП; последовательно, четко и логически стройно излагает материал, умеет тесно увязывать теорию с практикой; не затрудняется с ответами на проблемно-ориентированные вопросы; правильно обосновывает принятые решения;

- оценка «удовлетворительно» выставляется обучающемуся, если показал необходимый объем выполненных работ, но ответами на вопросы комиссии не может полно раскрыть сущность выполненной работы; непоследовательно излагает материал, не умеет тесно увязывать теорию с практикой; затрудняется с ответами на проблемно-ориентированные вопросы; допускает ошибки в обосновании принятых решений;

- оценка «неудовлетворительно» выставляется обучающемуся, который представил работу, но не ответил на вопросы комиссии по теме выполненной ВКР.

Решение о присвоении выпускнику квалификации «бакалавр» по направлению подготовки 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем (информационные технологии и электронная промышленность)» и выдаче диплома о высшем образовании государственного образца принимает государственная экзаменационная комиссия по положительным результатам итоговой государственной аттестации, оформленным протоколами экзаменационных комиссий.

Выпускнику, достигшему особых успехов в освоении основной образовательной программы и прошедшему все виды итоговых аттестационных испытаний с оценкой «отлично», сдавшему все учебные дисциплины и работы, внесенные в приложение к диплому, со средней оценкой 4,75 и не имеющему оценок «удовлетворительно», выдается диплом с отличием.

Решения государственной экзаменационной комиссии принимаются на закрытых заседаниях простым большинством голосов членов комиссий, участвующих в заседании при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов председатель комиссии (или заменяющий его заместитель председателя комиссии) обладает правом решающего голоса.

При оценке ВКР принимаются во внимание уровень теоретической и практической подготовки выпускников, их профессиональной подготовленности в соответствии с требованиями ФГОС ВО, установленные как на основе анализа качества выполненной ВКР, так и во время ее защиты. Оцениваются: актуальность и важность темы для науки и производства; выполнения по заказу производства; наличие публикаций по защищаемой теме.

Результаты защиты ВКР объявляются в тот же день после оформления протокола заседания ВКР. Каждая защита выпускной квалификационной работы оформляется отдельным протоколом.

Протоколы хранятся в учебном отделе учебно-методического управления и по истечении пяти лет передаются на хранение в архив университета. Выпускная квалификационная работа хранится в архиве университета.

Выпускнику, защитившему ВКР, решением ГЭК присваивается квалификация бакалавра по направлению 10.03.01 – Информационная безопасность, профиль «Безопасность автоматизированных систем (информационные технологии и электронная промышленность)».

Составители:
Зав.каф.ВТиЗИ — Т.З. Аралбаев
(должность) (расшифровка подписи)

(должность) (расшифровка подписи)

Заведующий кафедрой
вычислительной техники и защиты информации — Т.З. Аралбаев
(наименование кафедры) (подпись) (расшифровка подписи)

Председатель методической комиссии
10.03.01 Информационная безопасность — Т.З. Аралбаев
(код, наименование) (подпись) (расшифровка подписи)

Согласовано:
Декан факультета (директор института)
ФМИТ — С.А. Герасименко
(наименование факультета (института)) (подпись) (расшифровка подписи)

Заведующий отделом комплектования научной библиотеки — Н.Н. Бигалиева
(подпись) (расшифровка подписи)

Уполномоченный по качеству факультета — И.В. Крючкова
(подпись) (расшифровка подписи)