Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«____»_____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность объектов критической информационной инфраструктуры

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
2	*3*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен КР	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:
д.т.н.
профессор кафедры «Информационная безопасность
автоматизированных систем», В. А. Челухин

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой
ИБАС_____ А.Ю.Лошманов
(наименование кафедры) (подпись) (ФИО)

Заведующий выпускающей
кафедрой[1]_____
(наименование кафедры) (подпись) (ФИО)

[1] Согласовывается, если РПД разработана не на выпускающей кафедре.

1 Общие положения

Рабочая программа дисциплины «Информационная безопасность объектов критической информационной инфраструктуры» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Обеспечение информационной безопасности распределенных информационных систем» по направлению 10.05.03 "Информационная безопасность автоматизированных систем".

Задачи дисциплины	Изучить основные сведения по обеспечению безопасности объектов критической информационной инфраструктуры, научиться разрабатывать организационно-распорядительные документы по защите информации на объектах информатизации.
Основные разделы / темы дисциплины	Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Основные требования. Разработка организационных и технических мер, в соответствии с требованиями регуляторов

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Информационная безопасность объектов критической информационной инфраструктуры» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	З1(ПК-27) Основ законодательства по защите объектов ключевой инфраструктуры	У1(ПК-27) определять критические процессы и объекты на предприятии	Н1(ПК-27) разработки документации для объектов ключевой инфраструктуры
	З2(ПК-27) Порядка расчета категории значимости на объектах критической информационной инфраструктуры	У2(ПК-27) категорировать АСУТП как объекты ключевой инфраструктуры	

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность объектов критической информационной инфраструктуры» изучается на 2 курсе(ах) в 3 семестре(ах).

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к

базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик: Основы информационной безопасности.

Знания, умения и навыки, сформированные при изучении дисциплины «Информационная безопасность объектов критической информационной инфраструктуры», будут востребованы при изучении последующих дисциплин Разработка политики информационной безопасности, Аттестация объектов информатизации.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 з.е., 180 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	180
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	48
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	96
Промежуточная аттестация обучающихся – Экзамен КР	36

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Основные требования. Введение в тематику защиты значимых объектов критической информационной инфра-	8		16	26

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
структуры. Рекомендуемые к использованию в отрасли термины и определения. Понятие критической информационной инфраструктуры. Обсуждение актуальности тематики устойчивости функционирования объектов КИИ (ИС, ИТС, АСУ), относительно компьютерных атак. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Описание документов, которыми следует руководствоваться при обеспечении безопасности объектов КИИ. Принципы обеспечения безопасности критической информационной инфраструктуры. Система безопасности значимого объекта КИИ. Оценка безопасности критической информационной инфраструктуры. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Классификация автоматизированной системы управления проводится заказчиком или оператором в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления. Оценка последствий возможных аварий. Паспорт безопасности опасного производственного объекта. Декларация промышленной безопасности. Показатели критериев значимости объектов КИИ РФ и их значения. Сведения об объекте критической информационной инфраструктуры. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры. Возможные последствия в случае возникновения компьютерных инцидентов. Организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры. Обязанности и права субъектов КИИ.				

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Надзорная деятельность. Изменения в уголовном кодексе РФ и перечне сведений, составляющих гос. тайну. Взаимодействие с ГосСопка.				
Разработка организационных и технических мер, в соответствии с требованиями регуляторов (в данном разделе в рамках самостоятельной работы студентами выполняется КР) Организация общего порядка обеспечения безопасности значимых объектов КИИ. Установка требований к силам обеспечения безопасности значимых объектов КИИ. Обсуждение требований к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, требований к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов, требований по обеспечению безопасности значимых объектов КИИ РФ. Безопасность значимых объектов обеспечивается в соответствии со статьей 10 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Анализ угроз безопасности информации и разработка модели угроз безопасности информации или ее уточнение (при ее наличии). Проектирование подсистемы безопасности значимого объекта. Разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности). Классификация уязвимостей информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей ИС. Общие требования к структуре описания уязвимости. Методика оценки уязвимостей. Причины возникновения угроз безопасности информации. Основные признаки классификации угроз безопасности	8		16	70

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
информации. Систематический подход к определению угроз. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора конкретных средств защиты информации для реализации организационных и технических мер. Разработка АСУТП в целом, в том числе технического проекта, должна соответствовать общим требованиям, установленным ГОСТ 24.104 (АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ. Общие требования), а также требованиям, содержащимся в техническом задании на ее создание ГОСТ 34.602 (Техническое задание на создание автоматизированной системы). Последовательность стадий и этапов работ, связанных с определением целесообразности создания и собственно созданием АСУТП, определена в ГОСТ 34.601 (Автоматизированные системы стадии создания). Функционирование систем безопасности в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов критической информационной инфраструктуры, разрабатываемыми субъектами критической информационной инфраструктуры. ОРД по безопасности значимых объектов. Определяющие порядок и правила обеспечения безопасности значимых объектов КИИ. ОРД по безопасности значимых объектов. Определяющие порядок и правила функционирования системы безопасности значимых объектов (СБЗО) критической информационной инфраструктуры (КИИ).				
ИТОГО по дисциплине	**16**		**32**	**96**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	**Количество часов**
Изучение теоретических разделов дисциплины	20
Подготовка к занятиям семинарского типа	26
Подготовка и оформление КР	50
	96

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Челухин В.А. Информационная безопасность критической информационной инфраструктуры Российской Федерации. - [б. м.] : Издательские решения, 2020 - 106 с. ISBN 978-5-4498-5068-3 (Электронная версия).

2. Трещев И.А. Организационное и правовое обеспечение информационной безопасности. Изд. – Издательские решения ISBN 978-5-4496-4478-7, 2019 – 768с.

8.2 Дополнительная литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
2. Приказ ФСТЭК № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
3. Приказ ФСТЭК № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»;

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Информационная безопасность объектов информационной инфраструктуры» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и лабораторных занятий.

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента

Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к лабораторным занятиям, изучение теоретических разделов дисциплины, подготовка КР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Информационная безопасность объектов информационной инфраструктуры» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление КР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты КР;

Курсовая работа должна быть оформлена в соответствии с требованиями внутренних нормативных документов ФГБОУ ВО КнАГУ.

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при

осуществлении образовательного процесса по дисциплине

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

В данной дисциплине в рамках самостоятельной работы студенты выполняют курсовую работу.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению курсовой работы

Теоретическая часть курсовой работы выполняется по установленным темам с использованием практических материалов. К каждой теме курсовой работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои предложения. Общие положения должны быть подкреплены и пояснены конкретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+телеприёмник16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория №_202_, оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[2]
по дисциплине

Информационная безопасность объектов критической информационной инфраструктуры

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Обеспечение информационной безопасности распределенных информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2019*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
2	*3*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен КР	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[2] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

Код и наименование компетенции	Планируемые результаты обучения по дисциплине		
	Перечень знаний	Перечень умений	Перечень навыков
Профессиональные			
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	З1(ПК-27) Основ законодательства по защите объектов ключевой инфраструктуры	У1(ПК-27) определять критические процессы и объекты на предприятии	Н1(ПК-27) разработки документации для объектов ключевой инфраструктуры
	З2(ПК-27) Порядка расчета категории значимости на объектах критической информационной инфраструктуры	У2(ПК-27) категорировать АСУТП как объекты ключевой инфраструктуры	

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Показатели оценки**
Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Основные требования.	ПК-27	Лабораторная работа 1 Лабораторная работа 2 Лабораторная работа 3	Знание основных документов по объектам информационной инфраструктуры. Умение проводить категорирование и определять угрозы безопасности для объектов критической информационной инфраструктуры.
Разработка организационных и технических мер, в соответствии с требованиями регуляторов	ПК-27	Лабораторная работа 4 Лабораторная работа 5 КР	Умение разрабатывать организационно-распорядительные документы для объектов критической инфраструктуры

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
3 семестр ***Промежуточная аттестация в форме экзамена***				
1	Лабораторная работа 1 № 1	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 4 балла - студент выполнил задание, с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа № 2	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 8 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 6 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения в рамках освоенного учебного материала. 4 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	Лабораторная работа № 3	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 4 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удо-

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				влетворительные знания, навыки и умения в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
4	Лабораторная работа № 4	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 8 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 6 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения в рамках освоенного учебного материала. 4 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
5	Лабораторная работа № 5	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 4 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
Текущий контроль:			**35 баллов**	
Экзамен			**35 баллов**	
		Ответ на вопрос	20 баллов	20 баллов - студент правильно ответил на теоретический вопрос билета. Показал отличные знания, навыки и умения в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы. 15 баллов - *с*тудент ответил на теоретический вопрос билета с небольшими неточ-

Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
			ностями. Показал хорошие знания, навыки и умения в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов. 10 баллов - студент ответил на теоретический вопрос билета с существенными неточностями. Показал удовлетворительные знания, навыки и умения в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 0 баллов - при ответе на теоретический вопрос билета студент продемонстрировал недостаточный уровень знаний. При ответах на дополнительные вопросы было допущено множество неправильных ответов.
	Решение задачи	15 баллов	15 баллов - студент правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Ответил на все дополнительные вопросы. 10 баллов - студент выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Ответил на большинство дополнительных вопросов. 5 баллов - студент выполнил практическое задание билета с существенными неточностями. Показал удовлетворительные умения в рамках освоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 0 баллов - при выполнении практического задания билета студент продемонстрировал недостаточный уровень умений. При ответах на дополнительные вопросы было допущено множество неправильных ответов.
ИТОГО:		**70 баллов**	

Критерии оценки результатов обучения по дисциплине:
0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);
65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень);
75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень);
85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень).

3 семестр ***Промежуточная аттестация в форме*** КР
По результатам защиты курсового проекта (работы) выставляется оценка по 4-балльной шкале оценивания - оценка *«отлично»* выставляется студенту, если в работе содержатся элементы научного творчества и делаются самостоятельные выводы, достигнуты все результаты, указанные в задании, качество оформления отчета соответствует установленным в вузе требованиям и при защите студент проявил отличное владение материалом работы и способность аргументировано отвечать на поставленные вопросы по теме работы; - оценка *«хорошо»* выставляется студенту, если в работе достигнуты все результаты, указанные в задании, качество оформления отчета соответствует установленным в вузе требованиям и при защите студент проявил хорошее владение материалом работы и способность аргументировано отвечать на поставленные вопросы по теме работы; - оценка *«удовлетворительно»* выставляется студенту, если в работе достигнуты основные результаты, указанные в задании, качество оформления отчета в основном соответствует установленным в вузе требованиям и при защите студент проявил удовлетворительное владение материалом работы и способность отвечать на большинство поставленных вопросов по теме работы; - оценка *«неудовлетворительно»* выставляется студенту, если в работе не достигнуты основные результаты, указанные в задании или качество оформления отчета не соответствует установленным в вузе требованиям, или при защите студент проявил неудовлетворительное владение материалом работы и не смог ответить на большинство поставленных вопросов по теме работы.

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Примеры вариантов заданий (задания являются вымышленными и требуют согласования с преподавателем в части наличия тех или иных сведений). При необходимости преподаватель может внести изменения в формулировки вариантов, предложить дополнительные варианты. Обязательное требование выявление не менее 10 критических процессов и 15 угроз безопасности из банка данных угроз ФСТЭК РФ.

1. Автоматизированная система распределенной сети нефтезавода.
2. Автоматизированная система распределенной сети провайдера сети.
3. Автоматизированная система распределенной сети войсковой части.
4. Автоматизированная система распределенной сети атомной электростанции.
5. Автоматизированная система распределенной сети горнодобывающего комбината.
6. Автоматизированная система распределенной сети завода по производству самолетов.
7. Автоматизированная система распределенной сети аппарата президента.
8. Автоматизированная система распределенной сети подводных лодок.
9. Автоматизированная система распределенной сети гидроэлектростанции
10. Автоматизированная система распределенной сети метеостанции.

Лабораторная работа 1

По согласованию с преподавателем определить и оформить перечень критических объектов и процессов для данного предприятия.

Лабораторная работа 2

Для определенных процессов и объектов задать угрозы безопасности и определить методику оценки. Оформить приказ о создании комиссии по категорированию.

Лабораторная работа 3

Для определенных процессов и объектов в соответствии с методикой провести категорирование и оформить акт.

Лабораторная работа 4

Разработать и оформить модель угроз и модель нарушителя для объекта критической информационной инфраструктуры.

Лабораторная работа 5

В соответствии с требованиями Приказа ФСТЭК России от 25 декабря 2017 г. № 239 описать процедуру аудита объекта критической информационной инфраструктуры.

3.2 Задания для промежуточной аттестации в форме экзамена

Контрольные вопросы к экзамену

1. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Основные требования.
2. Основные вопросы защиты объектов критической информационной инфраструктуры. Термины и определения.
3. Понятие критической информационной инфраструктуры. Обсуждение актуальности тематики устойчивости функционирования объектов КИИ (ИС, ИТС, АСУ), относительно компьютерных атак.
4. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры.
5. Документы, которыми следует руководствоваться при обеспечении безопасности объектов КИИ.
6. Принципы обеспечения безопасности критической информационной инфраструктуры.
7. Система безопасности значимого объекта КИИ.
8. Оценка безопасности критической информационной инфраструктуры.
9. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.
10. Классификация автоматизированной системы управления в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.
11. Оценка последствий возможных аварий.
12. Паспорт безопасности опасного производственного объекта. Декларация промышленной безопасности.
13. Показатели критериев значимости объектов КИИ РФ и их значения.
14. Сведения об объекте критической информационной инфраструктуры. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры.
15. Возможные последствия в случае возникновения компьютерных инцидентов.
16. Организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры.
17. Обязанности и права субъектов КИИ. Надзорная деятельность.
18. Взаимодействие с ГосСопка.

19. Разработка организационных и технических мер, в соответствии с требованиями регуляторов
20. Организация общего порядка обеспечения безопасности значимых объектов КИИ.
21. Установка требований к силам обеспечения безопасности значимых объектов КИИ.
22. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, требований к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов, требований по обеспечению безопасности значимых объектов КИИ РФ.
23. Безопасность значимых объектов обеспечивается в соответствии со статьей 10 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
24. Анализ угроз безопасности информации и разработка модели угроз безопасности информации или ее уточнение (при ее наличии).
25. Проектирование подсистемы безопасности значимого объекта.
26. Разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности).
27. Классификация уязвимостей информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей ИС.
28. Общие требования к структуре описания уязвимости. Методика оценки уязвимостей. Причины возникновения угроз безопасности информации.
29. Основные признаки классификации угроз безопасности информации. Систематический подход к определению угроз.
30. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры.
31. Правила выбора конкретных средств защиты информации для реализации организационных и технических мер.
32. Разработка АСУТП в целом, в том числе технического проекта, должна соответствовать общим требованиям, установленным ГОСТ 24.104 (АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ. Общие требования), а также требованиям, содержащимся в техническом задании на ее создание ГОСТ 34.602 (Техническое задание на создание автоматизированной системы).
33. Последовательность стадий и этапов работ, связанных с определением целесообразности создания и собственно созданием АСУТП, ГОСТ 34.601 (Автоматизированные системы стадии создания).
34. Функционирование систем безопасности в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов критической информационной инфраструктуры, разрабатываемыми субъектами критической информационной инфраструктуры.
35. ОРД по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ.
36. ОРД по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов (СБЗО) критической информационной инфраструктуры (КИИ).

Типовые экзаменационные задачи

1. Определите является ли страховая компания объектом КИИ.
2. Если ни один из ОКВЭД организации не попал в сферы действия, указанные в п. 8 ст. 2 187-ФЗ, то следует ли отнести данную организацию и ее объекты к КИИ и почему. Что следует предпринять в данном случае?

Темы / задания курсовых проектов / курсовых работ

Тематика курсовых работ совпадает с темами лабораторных работ и является их продолжением. В ходе курсовой работы студентам предлагается оформить полный комплект документов на соответствующий объект критической информационной инфраструктуры в соответствии с перечнем указанным ниже. Часть документов студентами разрабатывается в ходе лабораторных работ.

1. Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (форма утверждена Приказом ФСТЭК России от 22 декабря 2017 г. № 236)
2. План проведения мероприятий по обеспечению безопасности значимых объектов КИИ
3. План реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, либо раздел в Регламенте по реагированию на инциденты информационной безопасности: «Информирование и взаимодействие с уполномоченными органами», где прописывается как осуществляется взаимодействие с регуляторами.
4. Документы по внедрению, приемке и эксплуатации средств. Порядок хранения и учета средств.
5. Документы по внедрению, приемке и эксплуатации средств. Порядок хранения и учета средств.
6. Регламент по реагированию на инциденты информационной безопасности
7. План по восстановлению функционирования, Правила резервного копирования
8. Приказ о создании комиссии
9. Перечень процессов в рамках функций (полномочий) или видов деятельности
10. Перечень критических процессов
11. Перечень объектов КИИ, подлежащих категорированию
12. Перечень возможных действий нарушителей в отношении объектов КИИ
13. Перечень угроз безопасности и уязвимостей программного обеспечения объектов КИИ
14. Акт (протокол работы комиссии) оценки возможных последствий
15. Акт категорирования объектов КИИ
16. Приказ о создании системы безопасности, назначении ответственных (подразделений) отвечающих за функции обеспечения безопасности КИИ, определении системы контроля
17. Приказ об определении функциональных обязанностей должностных лиц (подразделений), либо внесение корректировок в должностные инструкции ответственных работников.
18. Приказ о назначении ответственных за обеспечение безопасности значимых объектов КИИ
19. Регламент по повышению осведомленности персонала по вопросам обеспечения безопасности значимых объектов КИИ. Приложение. План проведения занятий.
20. Накладные на приобретение, сертификаты (для сертифицированных средств защиты информации), паспорт-формуляр, инструкции.
21. Инструкция оператору, пользователю, системному администратору
22. Политика, Положение, Регламент и т.п. определяющие порядок и правила обеспечения безопасности значимых объектов КИИ

23. Категорирование. Приказ о назначении комиссии. Положение (методика) о работе комиссии. План работы комиссии. Акт по результатам работы.
24. Результаты реализации мероприятий, проводимых для обеспечения безопасности значимого объекта на стадиях (этапах) его жизненного цикла, подлежат документированию. Состав и формы документов определяются субъектом критической информационной инфраструктуры.
25. Рекомендации по корректировке архитектуры значимого объекта и организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации;
26. Модель угроз безопасности информации для объекта КИИ или группы объектов КИИ.
27. Техническое задание (частное техническое задание);
28. Технический проект.
29. Описание архитектуры подсистемы безопасности значимого объекта;
30. Порядок и параметры настройки программных и программно- аппаратных средств, в том числе средств защиты информации;
31. Правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации)
32. Акт установки средств защиты
33. Правила (инструкции) безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами
34. Приказ по организации контроля физического доступа к программноаппаратным средствам значимого объекта и его линиям связи
35. Правила (Регламент) разграничения доступа, определяющие права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программноаппаратных средств
36. Приказ о назначении администратора безопасности значимого объекта
37. Порядок и План отработки действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.
38. Программа и методики предварительных испытаний работоспособности подсистемы безопасности значимого объекта и отдельных средств защиты информации,
39. Акт (протокол) оценки влияния подсистемы безопасности на функционирование значимого объекта при проектных режимах его работы
40. Приказ о вводе в опытную эксплуатацию значимого объекта и его подсистемы безопасности.
41. Программа и методики опытной эксплуатации, включая проверку функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер
42. Проверка знаний и умений пользователей и администраторов, необходимых для эксплуатации значимого объекта и его подсистемы безопасности (журнал или зачетная ведомость)
43. Программа и методики приемочных испытаний.
44. Акт приемки значимого объекта в эксплуатацию.
45. Приказ о вводе в действие значимого объекта и его подсистемы безопасности.
46. Приказ о назначении ответственных за выявление компьютерных инцидентов и реагирование на них.
47. Утверждение функциональных обязанностей
48. Инструкция по реагированию на компьютерные инциденты

49. План мероприятий по обеспечению безопасности значимого объекта на случай возникновения нештатных ситуаций;
50. Журнал (Зачетная ведомость) по обучению и отработке действий персонала по обеспечению безопасности значимого объекта в случае возникновения нештатных ситуаций;
51. Приказ об определении альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций;
52. Положение (Регламент) о резервировании программных и программно-аппаратных средств, в том числе средств защиты информации, каналов связи на случай возникновения нештатных ситуаций;
53. Приказ об обеспечении восстановления значимого объекта и (или) его компонентов в случае возникновения нештатных ситуаций;
54. Положение (Регламент) по проведению анализа возникших нештатных ситуаций и принятию мер по недопущению их повторного возникновения.

Дополнительно по необходимости (указывается преподавателем) так же необходимо разработать организационно-распорядительную документацию по взаимодействию с ГОССОПКА(в части использования средств криптографической защиты и средств предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты), а так же за взаимодействие и передачу сведений в ГОССОПКА

1. Приказ о создании системы обнаружения, предупреждения и ликвидации последствий компьютерных атак и назначении ответственных.
2. Функциональные обязанности должностных лиц (подразделений).
3. Правила (Регламент) реагирования на компьютерные инциденты.
4. Акт установки.
5. Накладные, формуляры, документация, сертификаты.
6. Инструкция оператору по эксплуатации средств.
7. Приказ об организации хранения средств.
8. Приказ об организации допуска на объекты КИИ должностных лиц федерального органа исполнительной власти.
9. Приказ об организации взаимодействия с ГосСОПКА
10. Приказ об утверждении перечня передаваемой информации
11. Приказ о порядке предоставления сведений
12. Приказ о назначении ответственного за организацию передачи сведений
13. Приказ об организации информационного обмена с субъектами КИИ
14. В Политике по информационной безопасности выделяются пункты, регламентирующие модернизацию, гарантийную и техническую поддержку средств защиты информации, либо разрабатывается отдельное положение (регламент).
15. Правила (Регламент) реагирования на компьютерные инциденты
16. Журнал учета компьютерных инцидентов
17. Приказ об организации взаимодействия с ГосСОПКА
18. Заявка на подключение и установку средств защиты
19. Информационное письмо в Национальный координационный центр после приема средств описанных ранее
20. Регламент по порядку доступа к средствам защиты
21. План ликвидации последствий компьютерных атак
22. План проведения тренировки сотрудников
23. Результаты анализа существующих инцидентов

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД
1	Windows 7+проектор. Изменено на Windows 7+телевизор Пр-л №10 от 4.10.2022 г.	Стр.13