МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
информатики
(наименование факультета полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
«03» 03 2023г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технические средства охраны

(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Безопасность автоматизированных систем»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2023

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность» на основании учебного плана ОПОП ВО 10.03.01 «Информационная безопасность», направленность «Безопасность автоматизированных систем», одобренного Ученым советом университета протокол № 7 «18» 02 2022 г.

Рабочая программа дисциплины обсуждена и рекомендована к применению в учебном процессе для обучения студентов по ОПОП ВО 10.03.01 «Информационная безопасность» на заседании кафедры информационной безопасности протокол № 7 «14» февраля 2023 г.,

Зав. кафедой ИБ Марухленко А.Л.

Разработчик программы
к.т.н., доцент кафедры ИБ Шевелев С.С.

Согласовано:

на заседании кафедры ИБ, протокол № 7 «14» февраля 2023 г.
Зав. кафедрой ИБ Марухленко А.Л.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 «Информационная безопасность», направленность «Безопасность автоматизированных систем», одобренного Ученым советом университета протокол №__ «__»_____ 202_г. на заседании кафедры «Информационной безопасности» №__ «___» _____ 202 _г.

Заведующей кафедрой
к.т.н., доцент Марухленко А.Л,

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 «Информационная безопасность», направленность «Безопасность автоматизированных систем», одобренного Ученым советом университета протокол №__ «__»_____ 202_г. на заседании кафедры «Информационной безопасности» №__ «___» _____ 202 _г.

Заведующей кафедрой
к.т.н., доцент Марухленко А.Л.

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Цель преподавания дисциплины

Дисциплина "Технические средства охраны" изучается с целью формирования у студентов знаний в области построения систем информационной безопасности с использованием технических средств охраны.

1.2 Задачи дисциплины

Основными задачами изучения учебной дисциплины являются приобретение студентами познаний в области:

– методах проектирования систем безопасности охраняемого объекта;

– изучение принципов построения систем охраны с использованием технических средств;

– изучение основных характеристик и параметров технических средств охраны;

– освоение методов и средств контроля эффективности технической охраны;

– критериев защищенности охраняемого объекта;

– экономической эффективности использования ТСО;

– виды угроз: совершение террористического акта, несанкционированное проникновение на территорию с целью завладения материальными ценностями, совершение нападений на руководителей и персонал.

– правильный подход к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисципли-ной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компе тенции	*наименование компетенции*		
ОПК-7	Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		**Знать:** источники угроз безопасности информации, методы оценки уязвимости информации, методы пресечения разглашения конфиденциальной информации, методы настройки, наладки программно-аппаратных комплексов, последовательность этапов обработки, при передаче данных в компьютерной сети. **Уметь:** отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства; применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации, анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов, применять программную среду Packet Tracer для построения сетей на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов, применять средства диагностики компьютерной сети, отслеживать перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. **Владеть:** навыками сопровождения и управления системами защиты информации, навыками проверки работоспособности программно-аппаратных комплексов.
ПК-3	Способностью администрировать подсистемы информационной безопасности объекта защиты		**Знать:** основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях. **Уметь:** использовать нормативную и правовую

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисципли-ной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компе тенции	*наименование компетенции*		
			документацию, характерную для информационной безопасности и методологии защиты инфокоммуникаций, анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем **Владеть:** навыками самостоятельной работы на компьютере и в компьютерныхсетях с целью выбора мер организационно правового обеспечения информационной безопасности сетей и систем связи, навыками проверки работоспособности программно-аппаратных комплексов, навыками разработки баз данных с учетом требований по обеспечению информационной безопасности, разработки комплекса мер для управления информационной безопасностью.
ПК-11	Способностью проводить эксперименты по заданной методике, обработ-ку, оценку погрешности и достоверности их результатов		**Знать:** свободно оперировать основными категориями управления и понимает связь между ними; о методах совместного достижения поставленной цели; в совершенстве знать методы инструментальной оценки уровня защищенности информационно -телекоммуникационных систем и объектов информатизации и нормы, использования программно-аппаратных средств обеспечения безопасности вычислительных систем, разработки баз данных с учетом требований по обеспечению информационной безопасности, разработки комплекса мер для управления информационной безопасностью. **Уметь:** применять понятийно – и категориальный аппарат при организации работы предприятия в нестандартных ситуациях; организовывать работу малого коллектива исполнителей в профессиональной деятельности; в совершенстве уметь проводить инструментальную оценку уровнязащищенности информационно-телекоммуникационных систем и

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисципли-ной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компе тенции	*наименование компетенции*		
			объектовинформатизации, разрабатывать прикладные программы, для создания защищенных информационных систем, применять средства обеспечения безопасности данных, проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети. **Владеть:** навыками организации работы малых коллективов в нестандартных ситуациях, навыками декомпозиции комплексных задач, в совершенстве владеть стандартным инструментарием для проведения инструментальной оценки уровня защищенности информационно-телекоммуникационных систем и объектов информатизации, навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня в области информационной безопасности, работы с программными средствами схемотехнического моделирования.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Технические средства охраны» относится к Дисциплина относится к дисциплинам вариативной части, дисциплинам по выбору (Б1.В.ДВ.08.01). Изучается на 3 курсе в 5 семестре

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

Общая трудоёмкость (объём) дисциплины составляет 5 зачётных единицы, 180 часов.

Таблица 3 – Объём дисциплины

Виды учебной работы	Всего часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72
в том числе:	
Виды учебной работы	Всего, часов
лекции	36
лабораторные занятия	36
практические занятия	не предусмотрено
Самостоятельная работа обучающихся (всего)	79,85
Контроль/экз (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
В том числе:	
зачет	не предусмотрено
зачет с оценкой	не предусмотрено
курсовая работа (проект)	не предусмотрено
экзамен (включая консультацию перед экзаменом)	1,15

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1.	Матрица безопасности объекта. Спектр угроз безопасности объекта.	Мероприятия по обеспечению безопасности объекта на первом этапе проектирования. Определение оборудование объекта техническими средствами защиты и организацию контрольно-пропускного режима. Угрозы в отношении персонала объекта, угрозы в отношении имущества, материальных ценностей и самого объекта, угрозы в отношении интеллектуального потенциала.
2.	Концепция защиты	Виды угроз: совершение террористического акта,

	объекта. Методологии разработки концепции комплексного обеспечения безопасности объектов охраны.	несанкционированное проникновение на территорию с целью завладения материальными ценностями, совершение нападений на руководителей и персонал. Определение стратегии комплексной безопасности. Определение стратегии комплексной безопасности. Обеспечение безопасности от физического проникновения на территорию и в помещения объекта. Защита от прогнозируемых к применению средств внегласного контроля. Защита от диверсионно-террористических средств. Человеческий фактор в системе обеспечения безопасности. Организация системы контроля доступа. Схема системы обеспечения безопасности объекта
3.	План нападения на объект. Содержание концепции защиты объекта.	Форма нападения: вооруженный налет, проникновение со взломом, внедрение прослушивающих устройств, выведение информации из компьютерных сетей, направление удара и варианты проникновения, привлекаемые силы и средства, время и продолжительность нападения, меры и силы прикрытия и поддержки, способы уничтожения следов и улик. Анализ возможных угроз и оценка степени риска, план здания, территория с указанием зон режимности, а также маршруты движения сотрудников и посетителей, схема охраны объекта: расположение и маршруты движения постов охраны, распределение функций между постами и ТСО. Рекомендации по организации контрольно-пропускного и внутри объектного режима. Рекомендации по порядку взаимодействия с правоохранительными органами. Принципы локализации происшествий и чрезвычайных ситуаций. Скелетная схема технического оснащения объекта.
4.	Классификация технических средств охраны, их основные тактико-технические характеристики и области применения.	Аппаратура ССОИ. Основные способы соединения станционной аппаратуры с периферийными блоками. Выбор структуры построения комплекса ТСО. Типы линий связи. Автономная система охраны. Системы с централизованным наблюдением. Классификация чувствительных элементов средств обнаружения. Виды взаимодействия чувствительных элементов со средой. Типовые подходы к классификации средств обнаружения и технических средств охраны
5.	Технические средства, используемые для увеличения эффективности охраны объекта	Средства задержки, средства охранной сигнализации, средства контроля доступа, приборы, регистрирующие пронос запретных материалов, средства наблюдения за помещениями и территорией, устройства, контролирующие правильность выполнения своих обязанностей должностными лицами, приборы ловушки, средства учета, накопления и обработки данных по вопросам безопасности
6.	Охрана удаленных объектов. Способ передачи информации с использованием радиоканала.	Структурная схема реализации охраны удаленного объекта. Структурная схема РПУ. Параметры передачи данных по радиоканалу. Датчики пожарно-охранной сигнализации (ПОС), модулятор, радиопередающее устройство, приемник, вычислительный комплекс
7.	Защита периметра охраняемого объекта. Разработка инженерных	Этапы проектирования. Выбор места расположения и строительства объекта. Особо охраняемые объекты. Использование природных особенностей местности: рельеф,

	сооружений защиты периметра	наличие водных преград при строительстве охраняемых объектов. Охрана периметра техническими средствами обнаружения: радиоволновые обнаружители, радиочастотные, оптические, акустические приборы; проводные системы защиты, вибрационные датчики, подземные сейсмические датчики, регистрирующие колебания почвы при движении нарушителя
8.	Системы видеонаблюдения. Комбинированная система видеонаблюдения	Особенности функционирования этой системы: круглосуточное функционирование с корректировкой чувствительности в зависимости от освещенности объекта в различное время суток; постоянная или временная видеозапись состояния объекта. Запись изображения включается при поступлении сигнала с датчика обнаружения, появлении в видеокадре любых изменений картинки. Сравнение цифровой и аналоговых систем видеонаблюдения. Основные принципы работы современных элементов видеокамер.
9.	Инженерные аспекты защиты непосредственно самого объекта	Инженерная защита здания. Специальное проектирование и защита коммуникаций: тоннелей водопроводного и сантехнического обеспечения, энергетических и телекоммуникационных каналов; разработка специальных углубленных фундаментов, дополнительное укрепление стен первых этажей от пролома; отсутствие на здании внешних лестничных проемов, предотвращающее проникновение через крышу; изоляция последнего этажа от чердачных помещений

Таблица 4.1.2 –Содержание дисциплины и её методическое обеспечение

№ Пп/п	Раздел (тема) дисциплины	Виды учебной деятельности (в часах)		Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек.	лаб.			
1	2	3	4	5	6	7
1.	Матрица безопасности объекта. Спектр угроз безопасности объекта.	2	4	У-1 МУ-1	УО-2	ОПК-7
2.	Концепция защиты объекта. Методологии разработки концепции комплексного обеспечения безопасности объектов охраны.	2	4	У-1, У-2 МУ-1	УО 1,2	ОПК-7, ПК-3
3.	План нападения на объект. Содержание концепции защиты объекта.	4	4	У-4 МУ-1	УО-3	ОПК-7

1	2	3	4	5	6	7
4.	Классификация технических средств охраны, их основные тактико-технические характеристики и области применения.	6	10	У-1, У-2 МУ-2	УО - 3 ЗЛР - 3	ОПК-7, ПК-3
5.	Технические средства, используемые для увеличения эффективности охраны объекта.	6	8	У-1, У-2 МУ-1	УО-5	ОПК-7
6.	Охрана удаленных объектов. Способ передачи информации с использованием радиоканала.	4	12	У-1, У-4 МУ-3	УО-5 ЗЛР-4	ОПК-7, ПК-11
7.	Защита периметра охраняемого объекта. Разработка инженерных сооружений защиты периметра.	4	8	У-3 МУ-3 МУ-4	УО-8	ОПК-7, ПК-3
8.	Системы видеонаблюдения. Комбинированная система видеонаблюдения.	4	10	У-4 МУ-5	УО-8 ЗЛР-6	ОПК-7, ПК-11
9.	Инженерные аспекты защиты непосредственно самого объекта.	4	12	У-6,7 МУ-6	УО-9 ЗЛР-7	ОПК-7, ПК-3
	Всего	36	72			

УО - устный опрос, ЗЛР – лабораторная работа

4.4. Лабораторные работы и практические занятия

4.2.1 Лабораторные занятия

Таблица 4.2.1 – Лабораторные занятия

№	Наименование лабораторного занятия	Объем, час.
1	2	3
1.	Знакомство с системой охраны JABLOTRON	6
2.	Программирование системы охраны JABLOTRON с ПК с использованием ПО Comlink	6
3.	Настройка GSM коммутатора	6
4.	Удаленное программирование с помощью мобильного телефона в режиме вызова и посредством смс-сообщений	6
5.	Программирование контрольной панели с помощью мобильного телефона	6
6.	Работа с системой видеонаблюдения VideoNET 8.0.	6
Итого**:**		36

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Матрица безопасности объекта. Спектр угроз безопасности объекта.	2 неделя	10
2.	Концепция защиты объекта. Методологии разработки концепции комплексного обеспечения безопасности объектов охраны.	3 неделя	10
3.	План нападения на объект. Содержание концепции защиты объекта.	5 неделя	12

4.	Классификация технических средств охраны, их основные тактико-технические характеристики и области применения.	8 неделя	10
5.	Технические средства, используемые для увеличения эффективности охраны объекта.	11 нед.	12
6.	Охрана удаленных объектов. Способ передачи информации с использованием радиоканала.	12 нед.	7,85
7.	Защита периметра охраняемого объекта. Разработка инженерных сооружений защиты периметра.	14 нед.	6
8.	Системы видеонаблюдения. Комбинированная система видеонаблюдения.	16 нед.	6
9.	Инженерные аспекты защиты непосредственно самого объекта.	18 нед.	6
Итого			79,85

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем6.разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– тем рефератов и докладов;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение лабораторной работы №2 «Программирование системы охраны JABLOTRON с ПК с использованием ПО Comlink»	Анализ конкретных ситуаций	4
2.	Выполнение лабораторной работы №2 «Настройка GSM коммутатора»	Анализ конкретных ситуаций	5
3.	Выполнение лабораторной работы №4 «Удаленное программирование с помощью мобильного телефона в режиме вызова и посредством смс-сообщений»	Анализ конкретных ситуаций	4
4.	Выполнение лабораторной работы №6 «Работа с системой видеонаблюдения VideoNET 8.0.»	Анализ конкретных ситуаций	5
	Итого		18

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
(ОПК-7) Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Управление информационной безопасностью. Информационные технологии. Практика по получению первичных профессионал ьных умений и навыков.	Безопасность сетей ЭВМ. Основы управления информационн ой безопасностью. Безопасность операционных систем. Безопасность сетей ЭВМ. Технические средства охраны. Системы контроля доступа и видеонаблюдения.	Программно-аппаратные средства защиты информации. Техническая защита информации. Сети и системы передачи информации. Администрировани е вычислительных сетей. Защита информационных процессов в компьютерных системах.
(ПК-3) Способностью администрировать подсистемы информационной безопасности объекта защиты	Введение в криптографию. Специализированно е программное обеспечения, информационные современные системы автоматического поиска для получения необходимой информации.	Аппаратные средства вычислительной техники. Криптографичес кие методы защиты информации. Безопасность сетей ЭВМ Технические средства охраны. Криптографические методы защит информации, программно-аппаратные средства защиты информации. Системы контроля доступа и видеонаблюдения. Технологическая практика.	Криптографические методы защит информации, программно-аппаратные средства защиты информации. Программно-аппаратные средства защиты информации. Инженерно- техническая защита информации. Эксплуатационн ая практика. Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.
(ПК-11) Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их	Практический подхода к разработке системы менеджмента качества и подготовки ее к сертификации, системный подход к разработке и	Проектирования подсистем и средств обеспечения информационной безопасности, реализации алгоритмов и используемых структур данных,	Специализированное программное обеспечение, информационные системы и ресурсы. Современные образовательные и информационные технологии.

результатов	внедрению систем менеджмента качества.	средствами языков программирования высокого уровня.	

**Этапы для РПД всех форм обучения определяются по учебному плану очной формы обучения следующим образом:*

Этап	Учебный план очной формы обучения/ семестр изучения дисциплины		
	Бакалавриат	Специалитет	Магистратура
Начальный	1-3 семестры	1-3 семестры	1 семестр
Основной	4-6 семестры	4-6 семестры	2 семестр
Завершающий	7-8 семестры	7-10 семестры	3-4 семестр

*** Если при заполнении таблицы обнаруживается, что один или два этапа не обеспечены дисциплинами, практиками, НИР, необходимо:*
– при наличии дисциплин, изучающихся в разных семестрах, – распределить их по этапам в зависимости от № семестра изучения (начальный этап соответствует более раннему семестру, основной и завершающий – более поздним семестрам);

– при наличии дисциплин, изучающихся в одном семестре, – все дисциплины указать для всех этапов.

Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на лабораторных и практических занятиях по темам лекций. В конце семестра – экзамен.

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Код компетенции/этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Уровни сформированности компетенции		
		Пороговый («удовлетворительно)	Продвинутый (хорошо»)	Высокий («отлично»)
1	2	**3**	**4**	**5**
(ОПК- 7) Способностью определять	Доля освоенных обучающимся	**Знать**: источники угроз безопасности	**Знать**: источники угроз безопасности	**Знать**: источники угроз безопасности информации,

информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД. Качество освоенных обучающимся знаний, умений, навыков.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	информации, методы оценки уязвимости информации, методы пресечения разглашения конфиденциальной информации, методы настройки, наладки программно-аппаратных комплексов. **Уметь**: отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации, анализировать техническую документацию, производить настройку, аладку и тестирование программно-аппаратных комплексов, применять программную среду Packet Tracer для построения сетей на разнообразном оборудовании в	информации, методы оценки уязвимости информации, методы пресечения разглашения конфиденциальной информации, методы настройки, наладки программно-аппаратных комплексов, последовательность этапов обработки. **Уметь**: отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации, анализировать техническую документацию, производить настройку, аладку и тестирование программно-аппаратных комплексов, применять программную среду Packet Tracer для построения сетей на разнообразном	методы оценки уязвимости информации, методы пресечения разглашения конфиденциальной информации, методы настройки, наладки программно-аппаратных комплексов, последовательность этапов обработки, при передаче данных в компьютерной сети. **Уметь**: отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства; применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации, анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов, применять программную среду Packet Tracer для построения сетей на разнообразном оборудовании в

		произвольных топологиях с поддержкой разных протоколов, применять средства диагностики компьютерной сети, отслеживать перемещение данных по сети. **Владеть**: формулирования комплекса мер по обеспечению информационной безопасности предприятия, навыками проверки работоспособности программно-аппаратных комплексов.	оборудовании в произвольных топологиях с поддержкой разных протоколов, применять средства диагностики компьютерной сети, отслеживать перемещение данных по сети, эксплуатировать и обслуживать системы охраны. **Владеть**: построения, монтажа и настройки с навыками сопровождения и управления системами защиты информации, навыками проверки работоспособности программно-аппаратных комплексовистем охраны.	произвольных топологиях с поддержкой разных протоколов, применять средства диагностики компьютерной сети, отслеживать перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства. **Владеть:** применения проектирования и эксплуатации систем охраны, навыками сопровождения и управления системами защиты информации, навыками проверки работоспособности программно-аппаратных комплексов.
1	2	**3**	**4**	**5**
(ПК-3) Способностью администрировать подсистемы информационной безопасности объекта защиты	Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД. Качество освоенных обучающимся знаний, умений, навыков. Умение применять	**Знать**: основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации,	**Знать**: основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации,	**Знать**: основные направления совершенствования правового обеспечения информационной безопасности сетей и систем связи, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основные

	знания, умения, навыки в типовых и нестандартных ситуациях	основные криптографические методы. **Уметь**: использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты инфокоммуникаций, анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем. **Владеть:** навыками самостоятельной работы на компьютере и в компьютерныхсетях с целью выбора мер организационно правового обеспечения информационной безопасности сетей и систем связи, навыками проверки работоспособности аппаратных комплексов, навыками разработки баз данных с учетом требований по обеспечению информационной безопасности.	основные криптографические методы, алгоритмы, протоколы. **Уметь**: использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты инфокоммуникаций, анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности. **Владеть:** навыками самостоятельной работы на компьютере и в компьютерныхсетях с целью выбора мер организационно правового обеспечения информационной безопасности сетей и систем связи, навыками проверки работоспособности программно-аппаратных комплексов, навыками разработки баз	криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях. **Уметь**: использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты инфокоммуникаций, анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. **Владеть:** навыками самостоятельной работы на компьютере и в компьютерныхсетях с целью выбора мер организационно правового обеспечения информационной безопасности сетей и систем связи, навыками проверки работоспособности программно-

			данных с учетом требований по обеспечению информационной безопасности.	аппаратных комплексов, навыками разработки баз данных с учетом требований по обеспечению информационной безопасности, разработки комплекса мер для управления информационной безопасностью.
(ПК-11) Способностью проводить эксперименты по заданной методике, обработ-ку, оценку погрешности и достоверности их результатов		**Знать:** свободно оперировать основными категориями управления и понимает связь между ними; о методах совместного достижения поставленной це-ли; в совершенстве знать методы инструментальной оценки уровня защищенности информационно - телекоммуникационных систем и объектов информатизации и нормы, использования программно-аппаратных средств обеспечения безопасности вычислительных систем, разработки баз данных. **Уметь:** применять понятийно – и	**Знать:** свободно оперировать основными категориями управления и понимает связь между ними; о методах совместного достижения поставленной цели; в совершенстве знать методы инструментальной оценки уровня защищенности информационно - телекоммуникационных систем и объектов информатизации и нормы, использования программно-аппаратных средств обеспечения безопасности вычислительных систем, разработки баз данных с учетом требований по обеспечению информационной безопасности. **Уметь:**	**Знать:** свободно оперировать основными категориями управления и понимает связь между ними; о методах совместного достижения поставленной цели; в совершенстве знать методы инструментальной оценки уровня защищенности информационно - телекоммуникационных систем и объектов информатизации и нормы, использования программно-аппаратных средств обеспечения безопасности вычислительных систем, разработки баз данных с учетом требований по обеспечению информационной безопасности, разработки комплекса мер для управления информационной

		категориальный аппарат при организации работы предприятия в нестандартных ситуациях; организовывать работу малого коллектива исполнителей в профессиональной деятельности; в совершенстве уметь проводить инструментальную оценку уровнязащищенности информационно-телекоммуникационных систем и объектовинформатизации, разрабатывать прикладные программы, для создания защищенных информационных систем, применять средства обеспечения безопасности данных. **Владеть:** навыками организации работы малых коллективов в нестандартных ситуациях, навыками декомпозиции комплексных задач, в совершенстве владеть стандартным инструментарием для	применять понятийно – и категориальный аппарат при организации работы предприятия в нестандартных ситуациях; организовывать работу малого коллектива исполнителей в профессиональной деятельности; в совершенстве уметь проводить инструментальную оценку уровнязащищенности информационно-телекоммуникационных систем и объектовинформатизации, разрабатывать прикладные программы, для создания защищенных информационных систем, применять средства обеспечения безопасности данных, проектировать и администрировать компьютерные сети. **Владеть:** навыками организации работы малых коллективов в нестандартных ситуациях, навыками декомпозиции комплексных	безопасностью. **Уметь:** применять понятийно – и категориальный аппарат при организации работы предприятия в нестандартных ситуациях; организовывать работу малого коллектива исполнителей в профессиональной деятельности; в совершенстве уметь проводить инструментальную оценку уровнязащищенности информационно-телекоммуникационных систем и объектовинформатизации, разрабатывать прикладные программы, для создания защищенных информационных систем, применять средства обеспечения безопасности данных, проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети. **Владеть:** навыками организации работы малых коллективов в нестандартных

		проведения инструментальной оценки уровня защищенности информационно-телекоммуникационных систем и объектов информатизации, навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня в области информационной безопасности.	задач, в совершенстве владеть стандартным инструментарием для проведения инструментальной оценки уровня защищенности информационно-телекоммуникационных систем и объектов информатизации, навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня в области информационной безопасности, работы с программными средствами.	ситуациях, навыками декомпозиции комплексных задач, в совершенстве владеть стандартным инструментарием для проведения инструментальной оценки уровня защищенности информационно-телекоммуникационных систем и объектов информатизации, навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня в области информационной безопасности, работы с программными средствами схемотехнического моделирования.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контроли-руемой	Технология формирова-ния	Оценочные средства		Описание шкал оценивания
				наимено вание	№№ заданий	
1	2	3	4	5	6	7
1.	Матрица безопасности объекта. Спектр угроз безопасности объекта	ОПК-7	Лекция, СРС	Вопросы для устного опроса	1	Согласно табл.7.2
2.	Концепция защиты объекта. Методологии разработки концепции комплексного обеспечения безопасности объектов охраны	ОПК-7	Лекция, СРС	Вопросы для устного опроса Защита лаб. раб №1	2	Согласно табл.7.2
3.	План нападения на объект. Содержание концепции защиты объекта	ОПК-7, ПК-3	Лекция, СРС, лабораторная работа№1	Вопросы для устного опроса КВЗЛР №2	3	Согласно табл.7.2
4.	Классификация технических средств охраны, их основные тактико-технические характеристики и области применения	ОПК-7, ПК-3	Лекция, СРС, лабораторная работа №2	Вопросы для устного опроса КВЗЛР №3	4	Согласно табл.7.2
5.	Технические средства, используемые для увеличения эффективности охраны объекта	ОПК-7	Лекция, СРС	Вопросы для устного опроса Защита лаб. раб №2	1-3	Согласно табл.7.2
6.	Охрана удаленных объектов. Способ передачи информации с использованием радиоканала	ОПК-7, ПК-11	Лекция, СРС, лабораторная работа №3	Вопросы для устного опроса КВЗЛР №3,4,5	5	Согласно табл.7.2

7.	Защита периметра охраняемого объекта. Разработка инженерных сооружений защиты периметра	ОПК-7, ПК-3, ПК-11	Лекция, СРС, лабораторная работа №4	Вопросы для устного опроса КВЗЛР № 5,6	6	Согласно табл.7.2
8.	Системы видеонаблюдения. Комбинированная система видеонаблюдения	ОПК-7, ПК-11	Лекция, СРС, лабораторная работа№5	Вопросы для устного опроса Защита лаб. раб №3	7	Согласно табл.7.2
9.	Инженерные аспекты защиты непосредственно самого объекта	ОПК-7, ПК-3, ПК-11	Лекция, СРС, лабораторная работа№6	Вопросы для устного опроса Защита лаб. раб №4	8	Согласно табл.7.2

СРС – самостоятельная работа студента, КВЗЛР – контрольные вопросы для защиты лабораторных работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы в тестовой форме по разделу (теме) 2. ««Варианты функционального назначения служебных помещений»

1. Охраняемые объекты делятся на наземные и подвижные.
2. Охраняемые объекты делятся на стационарные и подвижные.
3. Охраняемые объекты делятся на складские и производственные.
4. Охраняемые объекты делятся на наземные и подземные.

Вопросы для коллоквиума по разделу (теме 2) «Варианты функционального назначения служебных помещений»

1. Что определяет оборудование объекта техническими средствами защиты и организацию контрольно-пропускного режима
2. Анализ какого документа позволяет найти решения по обеспечению безопасности объекта на первом этапе проектирования
3. Как можно оценить защищённость по видам угроз
4. Какое мероприятие необходимо провести в конце проектирования охраны объекта
5. В чем заключается концепция защиты объекта

Темы рефератов

1. Электрошоковая Система охранной сигнализации периметра
2. Технические средства охранно-пожарной сигнализации
3. Система охранной сигнализации
4. Системы противопожарной автоматики
5. Система контроля и управления доступом
6. Охранные системы видеонаблюдения и видеорегистрации
7. Противокражевое оборудование
8. Система охранно-пожарной сигнализации, системы охраны периметра и инженерные заграждения
9. Особенности построения и тенденции развития современных технических средств охранной сигнализации
10. Классификация чувствительных элементов средств обнаружения
11. Основные направления защиты ценных ресурсов объекта от угроз
12. Радиоволновые и радиолучевые средства обнаружения

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся.
Промежуточная аттестация по дисциплине проводится в форме зачёта.

Промежуточная аттестация по дисциплине проводится в форме зачёта. Зачёт проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки(или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений,

навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Документы и инструкции плана по охране объекта.

А) Инструкций по охране объекта, схемы охраны, информации о порядке взаимодействия с ОВД, положении о пропускном и внутри объектовом режиме, табеля постам и боевого расчета.

Б) Состояние освещения территории объекта в ночное время.

В) Поэтажной схемой помещений с указанием их назначения и функционирования.

Г) С указанием мест возможного несанкционированного проникновения нарушителей на объект.

Задание в открытой форме:

Вопросы в открытой форме по разделу (теме) 2. «Варианты функционального назначения служебных помещений»

1. Какие существуют технические средства для увеличения эффективности охраны ……..
2. Какие технические средства регистрируют пересечение нарушителем заданных рубежей или появление нарушителя на объекте ……
3. Какую функцию выполняют средства задержки и защитные ограждения …
4. Какие посты охраны известны. Что такое средства контроля доступа …….
5. Какие устройства регистрируют пронос запрещенных предметов, материалов, изделий ……..
6. Как называются устройства регистрации событий и накопления информации …….

Задание на установление правильной последовательности, установить в каком порядке выполняется разработка функциональной схемы полного электронного ключа по заданной содержательной схеме алгоритма в микрооперациях:

1) Разработка структурной схемы электронногоключа устройства
2) Двоичное кодирование входных переменных
3) Вычисление результата при выполнении минимизации Картами Карно
4) Составление таблицы истинности электроного замка
5) Построение комбинационной схемы каскада полного электронного замка
6) Построение функциональной схемы электронного замка в заданном базисе
7) Моделирование функциональной схемы электронного замка в среде Multi-Sim
8) Оценка конструктивной сложности вычислительного устройства

Задание на установление соответствия: между классификациями цифровых вычислительных устройств электроннго замка

1	Цифровой двоичный электронный ключ	А	$R_i = \bar{Z}_{i+1}\bar{A}_iB_iV\bar{Z}_{i+1}A_i\bar{B}_i\ V\ Z_{i+1}\bar{A}_i\bar{B}_i\ VZ_{i+1}A_iB_i$
2	Функция цифрового двоичного ключа в минимизированной форме	Б	$S_i = \overline{P}_{i+1}\overline{A}_iB_i\ V\overline{P}_{i+1}A_i\overline{B}_i\ V\ P_{i+1}\overline{A}_i\overline{B}_i\ V\ P_{i+1}A_iB_i$
3	Перевод булевой функции в заданный базис	В	Функциональная схемая цифрового устройства в заданном базисе
4	Функция входных и выходных значений электронного ключа	Г	X= {x1, x2, x3, ...xn} F1 – двоичный код при котором происходит отпирание электронного ключа; F2 – минимизация булевых функций; F3 – реализация минимизированной функции в заданном базисе; F4 – Построение комбинационной схемы в среде МультиСим.

способов и видов информации

1	По способу кодирования	А	Числовая, символьная, графическая
2	По способу представления	Б	Световая, мультимедийная, комбинированная
3	По способу обработки	В	Сравнение, текстовая, графическая, числовая
4	По способу восприятия	Г	Визуальная, звуковая

Компетентностно-ориентированная задача:

Задать входные двоичные числа в прямом коде со старшим знаковым разрядом, составить таблицы истинности для полусумматора и полного сумматора, используя карты Карно определить функцию суммы Si и переноса Pi входных двоичных чисел, построить функциональную схему многоразрядного сумматора с последовательным переносом в заданном базисе, найти МОД.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016–2018 Обалльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Знакомство с системой охраны JABLOTRON»	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Программирование системы охраны JABLOTRON с ПК с использованием ПО Comlink»	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»

Выполнение лабораторной работы №3 «Настройка GSM коммутатора»	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение лабораторной работы №4 «Удаленное программирование с помощью мобильного телефона в режиме вызова и посредством смс-сообщений»	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение лабораторной работы №5 «Программирование контрольной панели с помощью мобильного телефона»	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение лабораторной работы №6 «Работа с системой видеонаблюдения VideoNET 8.0»	4	Выполнил, но «не защитил»	8	Выполнил и «защитил»
ВСЕГО	24		48	
Посещаемость	0		16	
Зачёт	0		36	
ИТОГО	24		100	

Для промежуточной аттестации, проводимой в форме тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ - 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение задачи – 6 баллов.
-

Максимальное количество баллов за тестирование - 36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная учебная литература

1. Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. – URL: https://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 20.03.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Грибунин, Вадим Геннадьевич. Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 416 с. – Текст : непосредственный.

3. Лопин, В. Н. Защита информации в компьютерных системах : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с. – Текст : непосредственный.

4. Тихонов, В. А. Информационная безопасность : концептуальные, правовые, организационные и технические аспекты : учебное пособие / В. А. Тихонов, В. В. Райх. - М. : Гелиос АРВ, 2006. - 528 с. : ил. - ISBN 5-85438-153-2 : 187.00 р. - Текст : непосредственный.

5. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 20.03.2023). – Режим доступа: по подписке. – Текст : электронный.

8.2. Дополнительная учебная литература

6. Пушкарев, В. П. Защита информационных процессов в компьютерных системах (безопасность жизнедеятельности 2) : учебное пособие / В. П. Пушкарев, В. В. Пушкарев ; Томский государственный университет систем управления и радиоэлектроники (ТУСУР). Кафедра средств радиосвязи (СРС). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2005. – 131 с. – URL: https://biblioclub.ru/index.php?page=book&id=208718 (дата обращения: 20.03.2023). – Режим доступа: по подписке. – Текст : электронный.

7. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. - М. : Академический Проект, 2003. - 640 с. - Текст : непосредственный.

8. Системы защиты информации в ведущих зарубежных странах : учебное пособие : / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. – URL: https://biblioclub.ru/index.php?page= book&id=93351 (дата обращения: 20.03.2023). – Режим доступа: по подписке. – Текст : электронный.

9. Зыков, С. В. Проектирование и разработка корпоративных информационных систем : учебное пособие / С. В. Зыков. - Москва : Ай Пи Ар Медиа, 2023. - 394 с. - URL: https://www.iprbookshop.ru/125021.html (дата обращения: 24.10.2022). – Режим доступа: по подписке. – Текст : электронный.

10. Информационные технологии : учебник / Ю. Ю. Громов, И. В. Дидрих, О. Г. Иванова [и др.] ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2015. – 260 с. – URL: https://biblioclub.ru/index.php?page= book&id= 444641 (дата обращения: 20.03.2023). - Режим доступа: по подписке. – Текст : электронный.

8.3. Перечень методических указаний

1. Знакомство с системой охраны JABLOTRON : методические указания для лабораторной работы для студентов укрупненной группы специальностей и направлений полготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А. Г. Спеваков. - Курск : ЮЗГУ, 2018. - 12 с. - Текст : электронный.

2. Программирование системы охраны JABLOTRON с ПК с использованием ПО Comlink : методические указания для лабораторной работы для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т ; сост. А. Г. Спеваков. - Курск : ЮЗГУ, 2018. - 10 с. - Текст : электронный.

3. Настройка GSM коммутатора : методические рекомендации для лабораторной работы для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. С. С. Шевелев. – Курск : ЮЗГУ, 2018. – 11 с. - Текст : электронный.

4. Удаленное программирование с помощью мобильного телефона в режиме вызова и посредством смс-сообщений : методические указания для лабораторной работы для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т ; сост. А. Г. Спеваков. - Курск : ЮЗГУ, 2018. - 14 с. - Текст : электронный.

5. Программирование контрольной панели с помощью мобильного телефона : методические рекомендации для работы для студентов укрупненной группы специальностей и направлений полготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. С. С. Шевелёв. – Курск : ЮЗГУ, 2018. – 9 с. - Текст : электронный.

6. Работа с системой видеонаблюдения VideoNET 8.0 : методические указания для лабораторной работы для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А. Г. Спеваков. – Курск : ЮЗГУ, 2018. – 17 с. - Текст : электронный.

8.4. **Другие учебно-методические материалы**

Периодические издания:

1. Журнал «Вопросы радиоэлектроники, сер. Электронная вычислительная техника»
2. Журнал «Вестник связи»
3. Журнал «Радио»
4. Журнал «Радиотехника»
5. Журнал «Радиотехника и электроника»
6. Журнал «Современная электроника»
7. Журнал «Сети и системы связи»
8. Журнал «Цифровая обработка сигналов»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
4. Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
5. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
6. Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
7. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
8. База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Технические средства охраны» являются лекции, лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные

с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Технические средства охраны»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Технические средства охраны» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Технические средства охраны» - закрепить теоретические знания,

полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Libreoffice, операционная система Windows, система видеонаблюдения VideoNET 8.0, система охраны «JABLOTRON», ПО Comlink

11. Материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска; система видеонаблюдения VideoNET 8.0, система охраны «JABLOTRON».

Для обеспечения учебного процесса используются: лекционная аудитория, оснащенная мультимедийными средствами, аудитория для практических занятий, компьютерная аудитория, обеспечивающая выход в ИНТЕРНЕТ.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в

письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых