

МИНОБРНАУКИ РОССИИ



Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЕ ДОСТУПОМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

Системы контроля и управление доступом
Рабочая программа дисциплины

Составитель(и):

Кандидат технических наук, доцент, зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации
№ 5 от 25.12.2025

ОГЛАВЛЕНИЕ

1. Пояснительная записка.....	4
1.1. Цель и задачи дисциплины.....	4
1.2. Формируемые компетенции, соотнесенные с планируемыми результатами обучения по дисциплине.....	4
1.3. Место дисциплины в структуре основной образовательной программы.....	5
2. Структура дисциплины.....	5
3. Содержание дисциплины.....	5
4. Образовательные технологии.....	8
5. Оценка планируемых результатов обучения.....	9
5.1. Система оценивания.....	9
5.2. Критерии выставления оценки по дисциплине.....	10
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.....	11
6. Учебно-методическое и информационное обеспечение дисциплины.....	13
6.1. Список источников и литературы.....	13
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».....	15
6.3. Профессиональные базы данных и информационно-справочные системы.....	15
7. Материально-техническое обеспечение дисциплины.....	15
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов.....	15
9. Методические материалы.....	16
9.1. Планы практических занятий.....	16
Приложение 1. Аннотация рабочей программы дисциплины.....	19

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности объекта охраны от физического доступа посторонних лиц с использованием системы контроля и управления доступа (СКУД).

Задачи дисциплины:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- изучение теоретических основ обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- формирование умений использовать современные достижения в области обеспечения безопасности объекта охраны от физического доступа посторонних лиц при реализации своей профессиональной деятельности;
- владение практическими навыками, применения современных методов, сил и средств контроля и управления доступом в обеспечении безопасности объекта охраны;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

1.2. Формируемые компетенции, соотнесенные с планируемыми результатами обучения по дисциплине

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-3 Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения	Знать: ~ требования нормативных и руководящих документов РФ по обеспечению безопасности объектов охраны от доступа посторонних лиц;
	ПК-3.2 Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации	Уметь: ~ анализировать состояние безопасности объекта охраны, разрабатывать нормативные документы по созданию и эксплуатации системы охраны объекта;
	ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного	Владеть: ~ навыками по использованию нормативных и руководящих документов в организации

	<i>обеспечения и последствий его функционирования</i>	<i>работ по защите объектов охраны;</i>
<i>ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</i>	<i>ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик</i>	<i>Знать: ~ требования нормативных и руководящих документов, методов, способов и технических решений по оборудованию объекта охраны от физического доступа посторонних лиц.</i>
	<i>ПК-6.2 Умеет оценить эффективность применяемых средств защиты информации с использованием штатных средств и методик</i>	<i>Уметь: ~ анализировать состояние защищённости объекта охраны, выявлять недостатки и устранять причины и факторы способствующих к появлению этих недостатков;</i>
	<i>ПК-6.3 Владеет навыками определения уровня защищенности и доверия средств защиты информации</i>	<i>Владеть: ~ навыками организации работы по применению и эксплуатации средств контроля и управления доступом на объекте охраны;</i>

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Системы контроля и управления доступом» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	26
3	Практические работы	36
	Всего:	64

Объем дисциплины в форме самостоятельной работы обучающихся составляет 44 академических часа.

3. Содержание дисциплины

Тема 1. Основные положения по защите объекта охраны. Факторы, влияющие на состояние защищенности объекта охраны, классификация нарушителя

Термины и определения, основные нормативные и правовые документы по техническим средствам охраны (ТСО), система контроля и управления доступом (СКУД).

Основные положения системного подхода к построению системы охраны объекта (СОО). Понятие системного подхода, основные методы при моделировании СОО, сущность системного подхода. Понятие СОО от физического доступа посторонних лиц, цели, задачи, принципы построения, основные показатели.

Объект защиты, классификация и категорирование объекта защиты. Факторы, влияющие на обеспечение безопасности объекта охраны от воздействия источников угроз. Исключение или минимизация случаев реализации угроз.

Эффективность системы охраны объекта, перечень факторов, влияющих на повышение эффективности системы. Факторы обеспечения безопасности объекта защиты от физического доступа посторонних лиц, несанкционированного вноса/выноса материальных и финансовых средств, носителей сведений конфиденциального характера, перечень субъективных и объективных факторов, которые влияют на эффективность защиты информации (такие как время реакции, задержки и нейтрализации источников угроз.).

Модель поведения нарушителя, классификация нарушителя, по его возможностям реализации угроз, физические параметры нарушителя, методы, способы и технические средства обхода, взлома рубежей охраны. Субъективные факторы, влияющие на возможность реализации угроз нарушителем.

Особенности охраны различных типов объектов с учетом наличия ценности и важности охраняемого материального имущества, носителей информации с различной степенью секретности или конфиденциальности.

Тема 2. Классификация системы контроля и управления доступом, назначение, основные и дополнительные задачи. Технические параметры

Классификация, назначение системы контроля и управления доступом (СКУД) в системе обеспечения безопасности объектов охраны. Цели, задачи СКУД, основные технические показатели и параметры СКУД.

Структура и основные технические компоненты СКУД. СКУД с ограниченными и расширенными функциями. Многофункциональные системы контроля и управления доступом. Механические, электромеханические, электрические СКУД. Системы контроля доступа физических лиц и контроля доступа к материальным и информационным носителям.

Критерии оценки СКУД. Государственный стандарт ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».

Типовые варианты СКУД и выполняемые ими основные и дополнительные задачи: управление потоками обслуживающего персонала, разделение потоков по территориальным зонам, по времени, контроль времени и зон (помещений) прохода отдельного работника, автоматическое управление доступом при возникновении определенных чрезвычайных ситуаций, (несанкционированное проникновение нарушителя в охраняемую зону, опасность пожара, радиационная опасность и т.д.), включение систем сигнализации и оповещения при возникновении чрезвычайной ситуации.

Тема 3. Идентификатор пользователя, устройства идентификации личности

Электронные идентификаторы: штрих-кодовые, магнитные карты, интеллектуальные (смарт-карты), «электронные таблетки», виганд-карточки, ключ-брелок «Touch memory», бесконтактные радиочастотные (PROXIMITY) карты и др.

Биометрические идентификаторы пользователя, статические, основанные на физиологических характеристиках человека (рисунки папиллярных линий пальцев, радужной оболочки глаз, капилляров сетчатки глаз, теплового изображения лица, геометрии

руки, ДНК), и динамические (почерк и динамика подписи, голос и особенности речи, ритм работы на клавиатуре) методы.

Назначение идентификаторов пользователя. Виды, принцип работы, технические характеристики. Сравнительный анализ идентификаторов пользователя, преимущества и недостатки идентификаторов пользователя. Достоинства и недостатки различных технологий идентификации пользователя

Считыватели для электронных идентификаторов. Виды считывателей: по типу эксплуатации, по методу обработки памяти, по типам идентификаторов. Считыватели карточек доступа контактные и бесконтактные.

Способы ввода считывания идентификационных признаков: ручной, контактный, дистанционный (бесконтактный) с определенного расстояния; с помощью биометрических

Тема 4. Контроллеры, назначение, технические параметры

Состав и назначение технических элементов контроллера. Контроллеры автономные и сетевые, контроллеры для распределенных систем контроля и управления доступом

Технические параметры контроллера: Количество точек прохода, объем базы данных пользователей, объем буфера событий, время работы системы при выключенном (зависшем, сгоревшем) компьютере, не теряя информации о событиях.

Комбинированные контроллеры выполняемые функции при наличии и отсутствии. связи или выхода из строя управляющего компьютера.

Смежные функции контроллеров: поддержка охранно-пожарной сигнализации, интеграции с подсистемами теленаблюдения, управлении некоторыми функциями оповещения и пожаротушения, возможность подключения к различными рабочими станциями и наличие доступа к сети Интернет.

Тема 5. Средства идентификации и аутентификации личности

Идентификационные карточки с магнитной дорожкой, аналоговые и цифровые. Идентификационные карточки с магнитной барий-ферритовой. Идентификационные карточки, кодированных по принципу Виганда. Бесконтактных радиочастотных (Proximity. Идентификационных карточках со скрытым штриховым кодом (Bar-кодом). Кодирование информации на идентификационных карточках с оптической памятью Голографические идентификационных карточек. Идентификационные карточки с искусственным интеллектом (Smart cards) Бесконтактные идентификационные карточки со встроенным миниатюрным приемопередатчик, Проксимити-идентификаторы (электронные пропуска в виде пластиковых карточек или брелков). Пластиковые ключи с использованием различных способов кодирования информации. Средства идентификации и аутентификации личности, принцип работы и их техническая реализация. Основные технические параметры средств идентификации и аутентификации личности, преимущества и недостатки.

Тема 6. Средства биометрической идентификации личности

Биометрическая СКУД. Статические и динамические методы биометрической идентификации личности.

Емкостные, потенциальные, тепловые и фоточувствительные сканеры для дактилоскопии.

Интеллектуальная технология распознавания лица (геометрия лица).

Биометрические терминалы. Идентификация с использованием лицевой термографии.

Принципы работы систем автоматической идентификации и слежения за лицами через телекамеры.

Системы идентификации по радужной оболочке и сетчатке глаза.

Системы идентификации по характеристикам голоса.

Варианты построение сетевой и автономной СКУД на базе биометрических устройств.

Перспективы развития биометрической идентификации личности

Тема 7. Исполнительные устройства, назначение, виды, принцип работы

Исполнительные устройства СКУД: назначение, состав, общие требования к установке

и эксплуатации.

Виды и принцип работы исполнительных устройств. Электрические замки и защелки, турникеты (обычные, настенные, раздвижные и т.п.) Шлюзовые камеры, тамбур-шлюзы. Ворота и шлагбаумы

Устройства заграждающие с исполнительными механизмами. Устройства заграждающие для задержки доступа людей. Устройства заграждающие для задержки доступа транспорта.

Требования к электропитанию и заземлению технических средств охраны.

Тема 8. Методические рекомендации по выбору и применению СКУД

Понятие о моделировании как основном процессе системного анализа. Виды моделей и их возможности при исследовании проблем охраны объекта защиты. Моделирование объекта защиты, возможных методов и способов обхода взлома СКУД.

Методические рекомендации по разработке системы безопасности объекта с использованием технических средств структурированию защищаемой информации. Организационные и технические меры по обеспечению режима безопасности объекта охраны.

Основные положения по повышению надёжности и отказоустойчивости СКУД. Показатели эффективности СКУД по охране объекта. Методы и технические решения по применению и использованию с целью повышения вероятности обнаружения источника угроз (нарушителя), исключения ложного срабатывания.

Оценка эффективности системы обеспечения охраны объекта с использованием СКУД.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Тема 1. Основные положения по защите объекта охраны. Факторы, влияющие на состояние защищённости объекта охраны, классификация нарушителя	Лекция 1. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
2.	Тема 2. Классификация системы контроля и управления доступом, назначение, основные и дополнительные задачи. технические параметры	Лекция 2. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
3.	Тема 3. Идентификатор пользователя, устройства идентификации личности	Лекция 3. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
4.	Тема 4. Контроллеры, назначение, технические параметры	Лекция 4. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
5.	Тема 5. Средства идентификации и аутентификации личности	Лекция 5. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.

6.	Тема 6. Средства биометрической идентификации личности	Лекция 6. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
7.	Тема 7. Исполнительные устройства, назначение, виды, принцип работы	Лекция 7. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
8.	Тема 8. Методические рекомендации по выбору и применению СКУД	Лекция 8. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
9.	Практическая работа № 1	Самостоятельная работа	Выполнение и защита практической работы Подготовка к защите ПР Консультация с использованием ЭП.
10.	Практическая работа № 2	Самостоятельная работа	Выполнение и защита практической работы Подготовка к защите ПР Консультация с использованием ЭП.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: – <i>опрос</i> – <i>выполнение и защита практических работ</i>	5 баллов 10 баллов	40 баллов 20 баллов
Промежуточная аттестация <i>зачет</i>		40 баллов
Итого за дисциплину <i>зачет</i>		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E

20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ А, В	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D, E	«удовлетворительн о»/ «зачтено (удовлетворительн о)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворител ьно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Основные положения и принципы построения системы охраны объекта защиты.	ПК-6
2.	Системный и комплексный подход к построению системы охраны объекта защиты.	ПК-3, ПК-6
3.	Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия.	ПК-6
4.	Модель поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия.	ПК-6
5.	Модель поведения нарушителя при использовании технических средств взлома, обхода СКУД.	ПК-6
6.	Условия, способствующие несанкционированному проникновению на объект защиты, методы и способы противодействия несанкционированному проникновению с использованием СКУД.	ПК-6
7.	Факторы, способствующие несанкционированному проникновению на объект защиты, методы и способы противодействия несанкционированному проникновению с использованием СКУД.	ПК-6
8.	Источники угроз, угрозы безопасности объектов защиты, степень нанесения ущерба в зависимости от реализации угроз.	ПК-6
9.	Объективные и субъективные факторы, способствующие проникновению на объект	ПК-6
10.	Модель поведения нарушителя. Классификация нарушителей, физические параметры нарушителя. методы и способы реализации угроз безопасности объектов защиты.	ПК-6
11.	Технические решения по защите КПП для пропуска лиц с использованием СКУД.	ПК-3, ПК-6
12.	Технические решения по защите КПП для пропуска автотранспорта с использованием СКУД.	ПК-3, ПК-6
13.	Назначение, задачи, модели СКУД	ПК-3, ПК-6
14.	Состав СКУД,	ПК-3
15.	Основные технические характеристики СКУД	ПК-3
16.	Представление модели разграничение доступа по зонам	ПК-6
17.	Требования при лицензировании и сертификации деятельности фирмы по охране объекта защиты.	ПК-6
18.	Нормативно-правовые документы, необходимые для разработки и эксплуатации СКУД.	ПК-6
19.	Электронные идентификаторы, виды.	ПК-3
20.	Штрих-кодовые идентификаторы, магнитные карты	ПК-3
21.	Интеллектуальные (смарт-карты), «электронные таблетки», виганд-карточки	ПК-3
22.	Бесконтактные радиочастотные (PROXIMITY) карты	ПК-3
23.	Ключ-брелок «Touch memoгу»	ПК-3
24.	Биометрические идентификаторы пользователя (виды)	ПК-3

25.	Идентификаторы, основанные на физиологических характеристиках человека (рисунки папиллярных линий пальцев, радужной оболочки глаз, капилляров сетчатки глаз, теплового изображения лица, геометрии руки, ДНК),	ПК-3
26.	Идентификаторы, основанные на физиологических динамических характеристиках человека	ПК-3
27.	Способы ввода считывания идентификационных признаков	ПК-3
28.	Организационные методы контроля эффективности защиты информации на примере вербального объекта.	ПК-3, ПК-6
29.	Технические методы контроля эффективности системы охраны объекта на примере вербального объекта.	ПК-3, ПК-6

Промежуточная аттестация (примерные вопросы к зачёту)

1. Основные положения концепции технической защиты информации.
2. Системный подход при построении системы защиты информации.
3. Цели и задачи принципы технической защиты объекта охраны.
4. Особенности защиты объекта охраны в системе обеспечения безопасности информации. Значение СКУД в системе защите объекта охраны.
5. Субъективные и объективные факторы влияющие на обеспечение защиты материальных ценностей и носителей информации от угроз воздействия. Значение СКУД на уменьшения влияния человеческого фактора.
6. Источники угроз, угрозы безопасности объекта, модель поведения нарушителя при несанкционированном проходе на объект защиты.
7. Классификация методов и способов охраны объекта. Структура системы охраны объекта от физического доступа посторонних лиц.
8. Современная концепция защиты объектов охраны от физического доступа посторонних лиц с использованием биометрических средств идентификации личности.
9. Виды СКУД для охраны объекта. Система автономной охраны. Система централизованной охраны.
10. Использование физических свойств нарушителя в практике обоснованного применения технических средств охраны.
11. Классификация СКУД по назначению, виду и решаемых задач.
12. Контроллеры СКУД. Назначение и классификация средств сбора и обработки информации.
13. Составные элементы системы контроля и управления доступом, их назначение и основные задачи.
14. Типы кодовых карт (пропусков) СКУД, принцип работы, технические характеристики, преимущества и недостатки.
15. Биометрические идентификация СКУД, виды, принцип работы, преимущества и недостатки.
16. Принципы организации интегрированных систем СКУД. Классификация и состав интегрированных систем СКУД.
17. Автономные контроллеры СКУД. сетевые контроллеры СКУД.
18. Идентификаторы (ключи touch memory, proximity-карточки, метки и брелоки).
19. Считыватели. идентификационных признаков, функции, устройство, принцип работы.
20. Считыватели карт доступа; RFID считыватели, «Proximity» считыватель. считыватель активных карт. считыватели смарт карт. Принцип работы, преимущества и недостатки.
21. Преграждающие устройства (электрозамки, турникеты, шлагбаумы и пр.), назначение виды, рекомендации по применению.
22. Устройства заграждающие с исполнительными механизмами.
23. Предложите варианты применения СКУД в магазине. Тип, состав, функциональные

- характеристики принцип работы СКУД, вид используемых идентификационных признаков
24. Предложите варианты применения СКУД в небольшом офисе. Тип, состав, функциональные характеристики принцип работы СКУД, вид используемых идентификационных признаков
 25. Предложите варианты применения СКУД в гостинице. Тип, состав, функциональные характеристики принцип работы СКУД, вид используемых идентификационных признаков
 26. Предложите варианты применения СКУД в производственном помещении. Тип, состав, функциональные характеристики принцип работы СКУД, вид используемых идентификационных признаков
 27. Требования к размещению и монтажу исполнительных устройств СКУДа. Требования к электропитанию и заземлению.
 28. Лицензирование и сертификация технических средств охраны и видеонаблюдения в области защиты информации.
 29. Основные этапы проектирования системы обеспечения безопасности объекта техническими средствами охраны и видеонаблюдения.
 30. Организационные и технические меры по обеспечению безопасности объекта с использованием технических средств охраны и видеонаблюдения.
 31. Порядок построения системы обеспечения безопасности объекта от физического доступа в соответствии с требованиями нормативных документов
 32. Способы оценки угроз безопасности информации и расходов на техническую защиту.
 33. Методика определения варианта оборудования объектов ТСО и СКУД в зависимости от категории объекта защиты.
 34. Определение вероятности перехвата нарушителей спроектированной системой охраны (ошибки 1 и 2 рода).
 35. Моделирование объекта защиты от физического доступа посторонних лиц.
 36. Моделирование угроз безопасности информации, возможных методов и способов реализации угроз.
 37. Контроль эффективности функционирования СКУД. Организационные, организационно-технические, технические методы контроля.

Примерные тестовые задания

1. Действительный идентификатор – это:

- а) идентификатор с идентификационным признаком, допускающий перемещение субъекта доступа через любую точку доступа в данный временной и календарный периоды
- б) идентификатор с идентификационным признаком, допускающий перемещение субъекта доступа через данную точку доступа в данный временной и календарный периоды*
- в) идентификатор с идентификационным признаком, допускающий перемещение субъекта доступа через любую точку доступа в любой временной и календарный периоды
- г) идентификатор с идентификационным признаком, допускающий перемещение любого субъекта доступа через любую точку доступа в данный временной и календарный периоды

2. Виды контроллеров СКУД:

- а) автономные, сетевые и многоуровневые
- б) автономные, сетевые и интегрированные*
- в) одноранговые, двухранговые и многоранговые

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Нормативно-правовые акты Российской Федерации

1. Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации от 05.12.2016 г. №646. [Электронный ресурс]: Режим доступа: <https://base.garant.ru/182535/>, свободный. - Загл. с экрана.

2. Федеральный закон РФ Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ. [Электронный ресурс]: Режим доступа: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

3. Рекомендации стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. [Электронный ресурс] : Режим доступа : <http://gostrf.com/normadata/1/4293850/4293850561.pdf>, свободный. – Загл. с экрана.

4. Р-064-2024 Методические рекомендации «Выбор и применение технических средств и систем контроля и управления доступом» – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2024. – 87 с. [Электронный ресурс] : Режим доступа : <https://nicohrana.ru/wp-content/uploads/2024/09/metodichka-skud.pdf>. – Загл. с экрана.

5. Р-102-2024 Методические рекомендации «Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации» – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2024. – 51 с. [Электронный ресурс] : Режим доступа : <https://nicohrana.ru/wp-content/uploads/2024/07/r-102-2024.pdf>. – Загл. с экрана.

6. Р-093-2024 Методические рекомендации «Обследование и прием под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации объектов, мест проживания и хранения имущества» – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2024. – 33 с. [Электронный ресурс] : Режим доступа : <https://nicohrana.ru/wp-content/uploads/2024/07/r-093-2024.pdf>. – Загл. с экрана.

7. Р 071-2017 Рекомендации «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения» – М.: ГУВО Росгвардии, 2017 – 20 с [Электронный ресурс] : Режим доступа : <https://nicohrana.ru/wp-content/uploads/2024/11/r-071-2017.pdf>. – Загл. с экрана.

8. ТП 78.36.005-2014 Типовой рабочий проект «Система контроля и управления доступом. Административное здание» – М.: ГУВО Росгвардии, 2014 – 37 с [Электронный ресурс] : Режим доступа : <https://nicohrana.ru/wp-content/uploads/2024/04/tp-78.36.005-2014-skud.pdf>. – Загл. с экрана.

9. ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» [Электронный ресурс]:
Режим доступа:
<http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=24963#02311715335921006>
3

Рекомендуемая литература (основная)

1. Ворона, В. А. Системы контроля и управления доступом / В.А. Ворона, В.А. Тихонов. - Москва : Гор. линия-Телеком, 2011. - 272 с.: ил.; . - (Обеспечение безопасности объектов). ISBN 978-5-9912-0059-2, 1000 экз. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/560195>. – Режим доступа: по подписке.

2. Системы контроля и управления доступом к объекту информатизации : учебное пособие / составители А. Г. Киренберг [и др.]. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2023. — 128 с. — ISBN 978-5-00137-426-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/399767>. — Режим доступа: для авториз. пользователей.

3. Якименко, А. А. Внедрение биометрической идентификации в системы контроля и управления доступом : учебное пособие / А. А. Якименко, В. В. Вихман. — Новосибирск : НГТУ, 2016. — 48 с. — ISBN 978-5-7782-3020-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/118227>. — Режим доступа: для авториз. пользователей.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Сайт НИЦ «Охрана» Росгвардии. - Режим доступа свобод.: <https://nicohrana.ru/normativno-tehnicheskaya-dokumentaciya/>
2. Официальный интернет-портал правовой информации - Режим доступа свобод.: <http://pravo.gov.ru>
3. Национальная электронная библиотека (НЭБ) www.rusneb.ru
4. ELibrary.ru Научная электронная библиотека www.elibrary.ru
5. Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3. Профессиональные базы данных и информационно-справочные системы

1. Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт

проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Практическая работа № 1 (10 ч). Обследование объекта

Цели работы:

- ознакомление с организацией обследования объектов на предмет инженерно-технической укреплённости элементов строительных конструкций;
- закрепление навыков выявления «уязвимых» с точки зрения несанкционированного проникновения мест и элементов строительных конструкций объектов;
- ознакомление с типовыми требованиями нормативных документов по организации инженерно-технической укреплённости элементов строительных конструкций охраняемых объектов;
- практическое освоение методов выработки предложений собственникам объектов по инженерно-технической укреплённости строительных конструкций охраняемых объектов.

Задания:

1. Изучить выданные в электронном виде:

- требования рекомендаций ГУВО Росгвардии Р-093-2024 и Р-102-2024;

- форму и пример составления акта обследования состояния технической укреплённости объекта (Р-093-2024).

2. Изучить выданные варианты планировок объектов с техническими описаниями их элементов технической укреплённости (в электронном виде, всего 17 вариантов).

Данные планировок с описаниями будут использованы и в последующих практических работах.

3. На основании Р-093-2024 и Р-102-2024, примера акта обследования, руководствуясь вышеуказанными требованиями по оформлению и содержанию актов, примером акта, определить категорию объекта и составить акт обследования состояния инженерно-технического укрепления объекта.

4. Разработать модель нарушителя с указанием вероятных маршрутов движения.

5. Составить отчёт о работе, в котором должны быть приведены план-схема объекта и акт осмотра объекта с рекомендациями об ИТУ объекта

Указания по выполнению заданий:

1. Преподаватель раздаёт в электронном виде рекомендации ГУВО Р-093-2024 и Р-102-2024, описания помещений и поэтажные схемы помещений (как вариант – студенты сами рисуют планы в MS Visio).

2. Ответить на вопросы при защите работы

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и выше.

Практическая работа № 2 (24 часа). Разработка предложений по оснащению объекта системой контроля и управления доступом.

Цели работы:

– ознакомление с организацией построения систем контроля и управления доступом, освоение навыков проектирования СКУД;

– закрепление навыков использования оборудования СКУД (считывателей, контроллеров, исполнительных устройств);

– ознакомление с аппаратурой компании Сек-Групп (НВП «Болид»).

Исходные данные:

– нормативный документ ГУВО Росгвардии Р 064-2017 «Выбор и применение систем контроля и управления доступом» в электронном виде;

– примеры проектной документации (типовой рабочий проект ТП 78.36.005-2014) в электронном виде;

– бюджет организации на создание СКУД (индивидуально для каждого студента).

– варианты планировок объектов с техническими описаниями их элементов технической укреплённости.

Порядок выполнения работы

1. Изучить выданные в электронном виде требования

– Р 064-2017;

– ТП 78.36.005-2014.

2. Изучить технические характеристики современных технических средств СКУД производства НВП «Болид» (<https://bolid.ru>) (лучше использовать данный сайт совместно с сайтом торговой компании Сек-Групп (<https://sec-group.ru/c/kontrol-dostupa/>), там, где невозможен выбор НВП «Болид» допускается выбирать оборудование других фирм (из списка Сек-Групп).

4. На основании Р 064-2017, изученного лекционного материала и примера составления проектной документации (выданного в электронном виде) составить по имеющимся вариантам планировок структурную схему, поэтажные планы сетей СКУД, пояснительную записку, расчёт ёмкости резервного питания (см. ТП 78.36.005-2014), спецификацию оборудования.

- 4.1. При составлении использовать MS Visio и поэтажный план, составленный на ЛР № 1.
- 4.2. При использовании СКУД торговой компании Сек-Групп (<https://sec-group.ru/c/kontrol-dostupa/>), в первую очередь НВП «Болид».
- 4.3. Система СКУД должна быть сетевой. Должны быть использованы:
 - идентификаторы
 - считыватели;
 - сетевые контроллеры;
 - преграждающие и исполнительные устройства (турникеты электрические замки, шлагбаумы, ограждения и т.д.).Выбор каждого типа устройства должен быть обоснован с технической и экономической точек зрения.
7. Оформить отчёт о практической работе, где привести:
 - план объекта размещением элементов СКУД (+отдельный файл в формате vsd);
 - экономический расчёт создания СКУД.

По результатам практических занятий обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённой формы связи.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности объекта охраны от физического доступа посторонних лиц с использованием системы контроля и управления доступом (СКУД).

Задачи:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- изучение теоретических основ обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- формирование умений использовать современные достижения в области обеспечения безопасности объекта охраны от физического доступа посторонних лиц при реализации своей профессиональной деятельности;
- владение практическими навыками, применения современных методов, сил и средств контроля и управления доступом в обеспечении безопасности объекта охраны от физического доступа посторонних лиц;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

В результате освоения дисциплины обучающийся должен:

Знать: требования нормативных и руководящих документов РФ по обеспечению безопасности объектов охраны от доступа посторонних лиц.

Уметь: анализировать состояние безопасности объекта охраны, разрабатывать нормативные документы по созданию и эксплуатации системы охраны объекта.

Владеть: навыками по использованию нормативных и руководящих документов в организации работ по защите объектов охраны.