МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»
профиль: Организация и технология защиты информации (по отрасли
или в сфере профессиональной деятельности)
Уровень квалификации выпускника (*бакалавр*)

Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Системы контроля и управления доступом
Рабочая программа дисциплины
Составитель:
д.т.н, профессор В.В. Арутюнов

Ответственный редактор
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Целью курса является формирование у студентов знаний по системам контроля и управления доступом, инженерно-техническим средствам охраны (СКУД и ИТСО) и формирование навыков работы по их использованию в системе защиты объекта от физического доступа посторонних лиц.

Задачи дисциплины: изучение факторов, влияющих на защиту объекта от физического несанкционированного доступа; определение категории объекта защиты; анализ принципов и основных требований по обеспечению безопасности объекта защиты; разработка технических решений и порядка проведения работ по оборудованию объекта защиты СКУД и ИТСО.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине *(модулю)*:

Компетенция (код и название)	**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: назначение и основные технические характеристики СКУД и ИТСО; Уметь: описывать объекты защиты; оценивать возможную величину ущерба от реализации угроз; Владеть: методикой по разработке законодательных, организационно-режимных и технических решений по обеспечению безопасности объекта защиты.
	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	Знать: угрозы безопасности информации программного обеспечения; Уметь: анализировать угрозы безопасности информации программного обеспечения; Владеть: навыками проверки соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации

	ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	Знать: о правилах ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования; Уметь: ликвидировать обнаруженное вредоносное программное обеспечение; Владеть: навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования.
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик	Знать: методы, способы и технические решения по оборудованию и эксплуатации СКУД и ИТСО; Уметь: определять рациональные меры, методы и технические решения применения СКУД и ИТСО для охраны объекта защиты; Владеть: навыками по выявлению возможных путей физического доступа на объект защиты посторонних лиц;
	ПК-6.2 Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	Знать: об эффективности мер, методов и технических решений применения СКУД и ИТСО; Уметь: оценивать эффективность используемых средств защиты информации на основе штатных средств и методик Владеть: навыками оценки эффективности применяемых средств защиты информации с использованием штатных средств и методик
	ПК-6.3 Владеет навыками определения уровня защищенности и доверия средств защиты информации	Знать: правила эксплуатации СКУД и ИТСО; Уметь: пользоваться правилами эксплуатации СКУД и ИТСО; Владеть: навыками выявления уровня защищённости и доверия средств защиты информации

1.3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Системы контроля и управления доступом» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины (модуля) необходимы компетенции, сформированные в ходе изучения следующих дисциплин и прохождения практики: "Организационное обеспечение информационной безопасности" и "Аппаратные средства вычислительной техники".

В результате освоения дисциплины (модуля) формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практики: "Технические средства охраны", "Комплексное обеспечение безопасности объекта информатизации - Организационное проектирование систем защиты информации".

2. Структура дисциплины (модуля)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 3 з.е., 114 ч., в том числе контактная работа обучающихся с преподавателем 60 ч., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Общая характеристика систем контроля и управления доступом	5	8		8			6	опрос
2	Основные типы устройств идентификации	5	6		6			6	опрос
3	Исполнительные устройства СКУД	5	4		8			8	опрос
4	Основные варианты реализации СКУД	5	6		10			10	опрос, контрольная работа
5	Экзамен						18	6	экзамен по билетам
	Итого		**24**		**36**		**18**	**36**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Общая характеристика систем контроля и управления доступом	Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Организация контрольно-пропускного режима на предприятии. Цели и задачи создания контрольно-пропускного режима. Подготовка исходных данных для организации контрольно-пропускного режима. Назначение, классификация и состав систем контроля и управления доступом (СКУД). Основные требования к системам контроля управления доступом. Особенности СКУД для крупных распределенных объектов.
2	Основные типы устройств идентификации	Основные средства идентификации и аутентификации. Кодонаборные устройства. Основные типы бесконтактных считывателей. Классификация и основные характеристики биометрических средств идентификации личности. Особенности реализации статических методов биометрического контроля. Идентификация по рисунку папиллярных линий. Особенности идентификация по радужной оболочке глаз. Идентификация по геометрии и тепловому изображению лица. Идентификация по рисунку вен руки. Особенности реализации динамических методов биометрического контроля. Идентификация по голосу и особенностям речи. Идентификация по ритму работы на клавиатуре.
3	Исполнительные устройства СКУД	Электрические замки и защелки в СКУД. Классификация турникетов в СКУД. Основные виды турникетов. Особенности полуавтоматических и автоматических шлюзовых кабин. Базовые типы шлюзовых кабин. Основные типы ворот и шлагбаумов. Автономные и сетевые контроллеры. Распределенные системы контроля и управления доступом. Исполнительные устройства СКУД российского производства.
4	Основные варианты реализации СКУД	Автономные СКУД. Сетевые системы контроля и управления доступом. Биометрические системы контроля и управления доступом. Интегрированные СКУД. Основные рекомендации по выбору средств и систем контроля доступа. Общие вопросы выбора СКУД. Выбор СКУД по техническим показателям. Выбор СКУД по экономическим показателям. Выбор биометрических СКУД.

4. Образовательные технологии

При реализации рабочей программы дисциплины используются следующие образовательные технологии:

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Общая характеристика систем контроля и управления доступом	Лекция 1 Практическое занятие 1	Вводная лекция с использованием видеопроектора опрос
2.	Основные типы устройств идентификации	Лекция 2 Практическое занятие 2	Лекция с использованием видеопроектора опрос
3.	Исполнительные устройства СКУД	Лекция 3 Практическое занятие 3	Лекция с использованием видеопроектора опрос
4.	Основные варианты реализации СКУД	Лекция 4 Практическое занятие 4 Контрольная работа	Лекция с использованием видеопроектора опрос Подготовка к контрольной с использованием материалов лекций и литературы

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: *- опрос* *- контрольная работа (темы 3-4)*	 *10 баллов* *20 баллов*	 *40 баллов* *20 баллов*
Промежуточная аттестация *(традиционная форма)*		*40 баллов*
Итого за семестр *экзамен*		*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/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
82-68/ C	зачтено	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	зачтено	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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	не зачтено	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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Примерная тематика опросного задания

1. Основные функции СКУД - ПК-3.
2. Базовые требования к СКУД - ПК-6.
3. Классификация СКУД - ПК-3.
4. Основные виды СКУД - ПК-3.
5. Выбор биометрических СКУД - ПК-6.
6. Общие вопросы выбора СКУД - ПК-6.
7. Разработка инструкции о контрольно-пропускном режиме - ПК-6.
8. Особенности сетевых систем контроля и управления доступом - ПК-3.

Примерная тематика контрольной работы

1. Особенности выбора СКУД по техническим показателям - ПК-6.
2. Характеристика сетевых контроллеров - ПК-3.
3. Базовые компоненты контроллеров СКУД - ПК-6.
4. Основные характеристики СКУД - ПК-3.
5. Понятие идентификатора пользователя - ПК-6.
6. Особенности распределённой структуры СКУД - ПК-3.
7. Основные типы устройств идентификации - ПК-3.
8. Особенности программного обеспечения для крупных СКУД - ПК-6.
9. Основные этапы биометрической технологии идентификации личности - ПК-3.
10. Особенности автономных СКУД - ПК-6.

Промежуточная аттестация (примерные контрольные вопросы по курсу)

1. Цели и задачи создания контрольно-пропускного режима - ПК-6.
2. Классификация систем контроля и управления доступом (СКУД) - ПК-3.
3. Состав СКУД - ПК-3.
4. Особенности СКУД для крупных распределенных объектов - ПК-6.
5. Основные средства идентификации и аутентификации - ПК-3.
6. Классификация биометрических средств идентификации личности - ПК-3.
7. Особенности реализации статических методов биометрического контроля - ПК-3.
8. Особенности идентификация по радужной оболочке глаз - ПК-3.
9. Классификация турникетов в СКУД - ПК-3.
10. Базовые типы шлюзовых кабин - ПК-6.
11. Особенности сетевых контроллеров СКУД - ПК-6.

12. Распределенные системы контроля и управления доступом - ПК-6.
13. Сетевые системы контроля и управления доступом - ПК-6.
14. Биометрические системы контроля и управления доступом - ПК-3.
15. Особенности интегрированных СКУД - ПК-3.
16. Основные рекомендации по выбору средств и систем контроля доступ - ПК-6.
17. Особенности выбора СКУД по техническим показателям - ПК-6.
18. Особенности выбора биометрических СКУД - ПК-6.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

а) источники:

1. ГОСТ Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний.- Режим доступа: URL: http://docs.cntd.ru/document/gost-r-54831-2011

2. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. - Режим доступа: URL: http://docs.cntd.ru/document/1200071688

б) основная литература:

1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html

2. Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html

в) дополнительная:

1. Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации. М.: Академия, 2010. - 510 с. - Режим доступа: URL: https://www.studmed.ru/sinilov-vg-sistemy-ohrannoy-pozharnoy-i-ohranno-pozharnoy-signalizacii_5fe6c9e0a2f.html

2. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. - М.: Горячая линия - Телеком, 2008. - 496 с. - Режим доступа: URL: https://yadi.sk/d/6uoIu6Pg3HEwS7

3. Танцеров А.Х. Инновации в системе контроля и управления доступом. В сборнике: Актуальные вопросы современной науки и образования. Сборник статей Международной научно-практической конференции: в 2 ч.. 2020. С. 54-56 — Режим доступа: URL: https://elibrary.ru/download/elibrary_41601138_16657388.pdf

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный портал в области защиты информации. - Режим доступа: URL:

http://www.securitylab.ru

2. Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru

3. Теория риска. - . Режим доступа: URL: http://risktheory.ru

4. Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru

Перечень БД и ИСС

№ п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Состав программного обеспечения (ПО)

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое

6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	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, регулируемыми эргономическими партами СИ-1;

- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Тема 1 (8 ч.). Организация контрольно-пропускного режима в организации

Вопросы для обсуждения:

1. Основные цели организации контрольно-пропускного режима на предприятии - ПК-6.
2. Базовые задачи организации контрольно-пропускного режима на предприятии - ПК-6.
3. Основные типы СКУД - ПК-3.
4. Классификация СКУД - ПК-3.
5. Что означает понятие " контрольно-пропускной режим" в организации? - ПК-3.
6. Типовые разделы инструкции о пропускном режиме - ПК-6.
7. Основные этапы подготовки исходных данных для организации контрольно-пропускного режима - ПК-6.
8. Соблюдение каких гарантий обеспечивает реализация контрольно-пропускного режима в организации? ПК-3.

Список источников и литературы:

ГОСТ Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний.- Режим доступа: URL: http://docs.cntd.ru/document/gost-r-54831-2011

ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. - Режим доступа: URL: http://docs.cntd.ru/document/1200071688

Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Горячая линия - Телеком. - 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html

Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации. М.: Академия. - 2010. - С. 10-21.

Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. - М.: Горячая линия - Телеком, 2008. - 496 с. - Режим доступа: URL: https://yadi.sk/d/6uoIu6Pg3HEwS7

Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru

Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru

Тема 2 (6 ч.). Биометрические методы и средства идентификации личности

Вопросы для обсуждения:

1. Основные методы биометрической идентификации и аутентификации - ПК-6.
2. Классификация биометрических средств идентификации личности - ПК-3.
3. Базовые этапы биометрической технологии идентификации личности - ПК-6.
4. Алгоритмы, используемые при обработке цифрового "отпечатка" папиллярных узоров пользователя - ПК-3.
5. Основные этапы идентификации личности человека по изображению лица - ПК-3.
6. В чём заключаются особенности повышения надежности распознавания личности при её идентификации по голосу? - ПК-3.
7. Основные методы борьбы с злоумышленниками, пытающимися подделать биометрический идентификатор пользователя - ПК-6.
8. Особенности идентификация по радужной оболочке глаз - ПК-3.
9. Особенности повышения надежности распознавания личности при её идентификации по голосу - ПК-6.

Список литературы:

Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html

Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html

Танцеров А.Х. Инновации в системе контроля и управления доступом. В сборнике: Актуальные вопросы современной науки и образования. Сборник статей Международной научно-практической конференции: в 2 ч.. 2020. С. 54-56 — Режим доступа: URL: https://elibrary.ru/download/elibrary_41601138_16657388.pdf

Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru

Теория риска. - . Режим доступа: URL: http://risktheory.ru

Национальный открытый университет ИНТУИТ. - Режим доступа: URL:

http://www.intuit.ru

Тема 3 (4 ч.). Характеристика исполнительных устройств

Вопросы для обсуждения:

1. Схема разветвленной сети СКУД - ПК-3.
2. Базовые виды сетевых - ПК-6.
3. Основные требования к структуре и возможностям СКУД - ПК-3.
4. Особенности распределенных систем контроля и управления доступом - ПК-6.
5. Классификация средств контроля и управления - ПК-6.
6. В состав какого класса средств контроля и управления доступа входят исполнительные устройства? - ПК-6.
7. Основные классы исполнительных устройств - ПК-3.
8. Классификация турникетов как исполнительных устройств - ПК-3.

Список литературы:

Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html

Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html

Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru

Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru

Тема 4 (4 ч.). Основные рекомендации по выбору средств и систем контроля доступа

Вопросы для обсуждения:

1. Общие вопросы выбора СКУД - ПК-6.
2. Характеристика автономных СКУД - ПК-3.
3. Основные преимущества интегрированных СКУД - ПК-3.
4. Базовые рекомендации по выбору средств и систем контроля доступа - ПК-6.
5. Почему отечественные разработки СКУД более предпочтительны для организации? - ПК-3.
6. Особенности выбора СКУД для крупных организаций - ПК-6.
7. Чем различаются условный и оперативный эффект от внедрения СКУД? - ПК-3.
8. Отличительные особенности выбора биометрических СКУД - ПК-6.

Список литературы

Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html

Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html

Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации. М.: Академия, 2010. - 510 с. - Режим доступа: URL: https://www.studmed.ru/sinilov-vg-sistemy-ohrannoy-pozharnoy-i-ohranno-pozharnoy-signalizacii_5fe6c9e0a2f.html

Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru

Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru

Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru.

9.2. Методические рекомендации по организации самостоятельной работы

Вид работы	**Содержание (перечень вопросов)**	**Трудоемкость самостоятельной работы (в часах)**	**Рекомендации**
Подготовка к практическому занятию Тема 1. «Организация контрольно-пропускного режима в организации»	Что означает понятие "контрольно-пропускной режим" в организации? Типовые разделы инструкции о пропускном режиме. Основные этапы подготовки исходных данных для организации контрольно-пропускного режима. Соблюдение каких гарантий обеспечивает реализация контрольно-пропускного режима в организации?	6	Проанализировать материал из законодательных, нормативных документов, учебников: ГОСТ Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний.- Режим доступа: URL: http://docs.cntd.ru/document/gost-r-54831-2011 ГОСТ Р 51241-2008 Средства и системы контроля и управления

			доступом. Классификация. Общие технические требования. Методы испытаний. - Режим доступа: URL: http://docs.cntd.ru/document/1200071688 Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Горячая линия - Телеком. - 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации. М.: Академия. - 2010. - С. 10-21. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. - М.: Горячая линия - Телеком, 2008. - 496 с. - Режим доступа: URL: https://yadi.sk/d/6uoIu6Pg3HEwS7 Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru
Подготовка к практическому занятию Тема 2 «Биометрические методы и средства идентификации личности»	Классификация биометрических средств идентификации личности. Базовые этапы биометрической технологии идентификации	6	Проанализировать материал из законодательных, нормативных документов, учебников: Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.:

	личности. Алгоритмы, используемые при обработке цифрового "отпечатка" папиллярных узоров пользователя. Основные этапы идентификации личности человека по изображению лица.		Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html Танцеров А.Х. Инновации в системе контроля и управления доступом. В сборнике: Актуальные вопросы современной науки и образования. Сборник статей Международной научно-практической конференции: в 2 ч.. 2020. С. 54-56 — Режим доступа: URL: https://elibrary.ru/download/elibrary_41601138_16657388.pdf Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru Теория риска. - . Режим доступа: URL: http://risktheory.ru Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru
Подготовка к практическому занятию Тема 3 «Характеристика исполнительных устройств»	Схема разветвленной сети СКУД. Базовые виды сетевых контроллеров. Основные требования к структуре и возможностям СКУД.	8	Проанализировать материал из законодательных, нормативных документов, учебников: Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. -

	Особенности распределенных систем контроля и управления доступом.		М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru
Подготовка к практическому занятию Тема 4 «Основные рекомендации по выбору средств и систем контроля доступа»	Общие вопросы выбора СКУД. Характеристика автономных СКУД. Основные преимущества интегрированных СКУД. Базовые рекомендации по выбору средств и систем контроля доступа.	10	Проанализировать материал из законодательных, нормативных документов, учебников: Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html Волхонский В.В. Системы контроля и управления доступом. - СПб: Университет ИТМО, 2015. - 200 с. - Режим доступа: URL: https://fileskachat.com/view/33860_fc60975fb4dd7daf7df441072dc70d31.html

			Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации. М.: Академия, 2010. - 510 с. - Режим доступа: URL: https://www.studmed.ru/sinilov-vg-sistemy-ohrannoy-pozharnoy-i-ohranno-pozharnoy-signalizacii_5fe6c9e0a2f.html Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru Информационный портал ФСТЭК. - Режим доступа: URL: http://www.fstec.ru Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru.

Приложение 1

АННОТАЦИЯ

Дисциплина «Системы контроля и управления доступом» реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Целью курса является формирование у студентов знаний по системам контроля и управления доступом, инженерно-техническим средствам охраны (СКУД и ИТСО) и формирование навыков работы по их использованию в системе защиты объекта от физического доступа посторонних лиц.

Задачи: изучение факторов, влияющих на защиту объекта от физического несанкционированного доступа; определение категории объекта защиты; анализ принципов и основных требований по обеспечению безопасности объекта защиты; разработка технических решений и порядка проведения работ по оборудованию объекта защиты СКУД и ИТСО.

Дисциплина направлена на формирование следующих компетенций:

- ПК-3 - способен администрировать подсистемы информационной безопасности объекта защиты;

В результате освоения дисциплины обучающийся должен:

- Знает требования к встроенным средствам защиты информации программного обеспечения
- 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
- Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования

- ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

В результате освоения дисциплины обучающийся должен:

- Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик
- Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик
- Владеет навыками определения уровня защищенности и доверия средств защиты информации

По дисциплине (модулю) предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.