

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 комплексной защиты информации

БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(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 2024

БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
Рабочая программа дисциплины

Составитель:

Кандидат технических наук, доцент, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор

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

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации
№ 8 от 14.03.2024 г.

Оглавление

1	Пояснительная записка.....	4
1.1	Цель и задачи дисциплины	4
1.2	Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:.....	4
1.3	Место дисциплины в структуре образовательной программы	5
2	Структура дисциплины.....	5
3	Содержание дисциплины	6
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.....	11
6.1	Список источников и литературы	11
6.2	Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ..	13
6.3	Профессиональные базы данных и информационно-справочные системы	13
7	Материально-техническое обеспечение дисциплины	14
8	Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья.....	14
9	Методические материалы.....	16
9.1	Планы практических занятий	16
	<i>Приложение 1. Аннотация рабочей программы дисциплины.....</i>	<i>18</i>

1 Пояснительная записка

1.1 Цель и задачи дисциплины

Цель дисциплины: развить у слушателей подход к решению технических задач программно-аппаратной защиты информации.

Задачи: формирование у студентов представлений об инфраструктуре критически важных информационных систем, научить студентов использовать механизмы обеспечения юридической значимости документов.

1.2 Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать нормативные правовые документы в области защиты информации, основные проектные решения, средства и методы защиты информации от несанкционированного доступа.
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	Уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты, анализировать защищаемые активы в зависимости от специфики от системы обработки информации ограниченного доступа
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	Владеть навыками по реализации политик информационной безопасности и технологических проектов в области ИБ
ПК-4 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК-4.1 Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	Знать: методы и способы обеспечения отказоустойчивости АС, основы администрирования защищенных АС и подсистем безопасности объектов КИИ РФ

	<p>ПК-4.2 Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах</p>	<p>Уметь: применять и настраивать типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости для объектов КИИ с учетом требований 178 ФЗ и 31 Приказа ФСТЭК.</p>
	<p>ПК-4.3 Владеет навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций</p>	<p>Владеть: Навыками обнаружения и устранения неисправности работы, своевременное и оперативное реагирование на внештатные ситуации, умениями настраивать отказоустойчивый кластер с подсистемой “горячего” резервирования</p>

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность критически важных информационных систем» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: «Безопасность операционных систем», «Программно-аппаратные средства защиты информации», «Безопасность программного обеспечения автоматизированных систем», «Защита от несанкционированного доступа к информации в автоматизированных системах».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: «Проектирование защищенных автоматизированных систем», «Производственная практика (Преддипломная практика)».

2 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 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
7	Лекции	28
7	Практические работы	32
Всего:		60

Объем дисциплины в форме самостоятельной работы обучающихся составляет 48 академических часа.

3 Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Компоненты инфраструктуры критически важных информационных систем	Основные понятия. Методология. Компоненты инфраструктуры критически важных информационных систем.
2	Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов	<p>Требования регулятора. Изучение нормативно-правовых документов. В стратегию национальной безопасности РФ 2020 включен следующий пункт: угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.</p> <p>Здесь интересным моментом и отправной точкой дальнейшего моего повествования служит сочетание «совершенствование безопасности функционирования» ИС КВО</p>
3	Структура современных критически важных информационных систем	<p>В соответствии с распоряжением Правительства РФ от 23.03.2006 № 411-р к критически важным относятся совершенно разные по своему назначению объекты — магистральные сети связи, системы телерадиовещания, заводы, электростанции, предприятия нефте- и газодобычи, транспортная инфраструктура и т. п. Столь различные объекты имеют слишком разные ИТ-системы, поэтому универсальных критериев защищенности ИТ-инфраструктур КВО скорее всего не существует — они должны определяться для КВО, сходных по назначению и архитектуре.</p> <p>Системы SCADA включают в себя средства приема и обработки критически важной информации (сигналов тревоги, измерений и команд), которая поступает с удаленных подстанций, представляющих собой автоматизированные системы, напичканные различным оборудованием: периферийные терминалы, программируемые</p>

		<p>контроллеры и датчики. Связь с подстанциями двухсторонняя — они могут получать управляющие команды, которые исполняются с помощью сервомеханизмов. В этой структуре ИКТ играют важнейшую роль: в частности, дистанционное получение данных и наблюдение в реальном времени часто осуществляется с помощью Интернета и веб-интерфейсов. Как следствие, появились новые стандарты на коммуникационные протоколы SCADA, такие как Modbus-TCP, Distributed Network Protocol (DNP3), IEC-60870-5-104 и InterControl Center Protocol (ICCP, IEC60870-6), регулирующие автоматизацию и управление, а также порядок соединения систем SCADA друг с другом.</p>
4	<p>Особенности подходов и методов в области защиты критически важных информационных систем</p>	<p>Наивысший приоритет в защите ИТ-инфраструктур КВО имеют: защита периметра; разграничение доступа к критичным серверам; защита серверов управления и рабочих станций, которые управляют АСУ ТП; защита критичных контроллеров АСУ ТП. Обеспечение их ИБ позволяет нивелировать последствия большинства угроз.</p>
5	<p>Использование средств защиты информации</p>	<p>14 марта 2014 года ФСТЭК России выпустил Приказ N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».</p> <p>Данный документ устанавливает требования к обеспечению защиты информации: от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.</p> <p>Приказ №31 регламентирует:</p> <ul style="list-style-type: none"> • Разработку и документирование правил и процедур (политик) обеспечения безопасности; • Требования к защите среды виртуализации; • Обучение и отработку действий пользова-

		<p>телей в случае возникновения нештатных (непредвиденных) ситуаций;</p> <ul style="list-style-type: none"> • Требования по безопасной разработке ПО; • Требования по инцидент-менеджменту и анализу угроз безопасности; • И другие факторы, обеспечивающие должный уровень безопасности объектов. <p>Учитывая важность объектов и величину ущерба, который может быть нанесен окружающей среде и здоровью людей, требования Приказа №31 направлены на обеспечение функционирования АСУ технологическими процессами в штатном режиме, при котором обеспечивается соблюдение проектных значений параметров выполнения целевых функций автоматизированной системы управления в условиях воздействия угроз безопасности информации, а также на снижение рисков незаконного вмешательства в процессы функционирования автоматизированных систем управления критически важных объектов, безопасность которых обеспечивается в соответствии с законодательством Российской Федерации.</p> <p>В автоматизированной системе управления объектами защиты являются:</p> <ul style="list-style-type: none"> • Информация о параметрах (состоянии) управляемого объекта или процесса, управляющая информация, контрольно-измерительная информация, иная критически важная (технологическая) информация; • Программно-технический комплекс, включающий технические средства, программное обеспечение, а также средства защиты информации.
--	--	---

4 Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Компоненты инфраструктуры критически важных информационных систем	Лекция 1 Практическое занятие 1. Самостоятельная работа	Традиционная с использованием презентаций, тестирование Выполнение задания Изучение материалов лекций
2	Нормативно-методическая база использования электрон-	Лекция 2 Практическое занятие 2.	Традиционная с использованием презентаций Выполнение задания

	ной подписи для придания юридической значимости электронных документов	Самостоятельная работа	Изучение материалов лекций
3	Структура современных критически важных информационных систем	Лекция 3.1 Лекция 3.2 Практическое занятие 3. Самостоятельная работа	Традиционная с использованием презентаций, тестирование Выполнение задания Изучение материалов лекций
4	Функции удостоверяющего центра	Лекция 4.1 Лекция 4.2 Практическое занятие 4 Самостоятельная работа	Традиционная с использованием презентаций, тестирование Выполнение задания Изучение материалов лекций
5	Использование функций провайдера криптографических услуг	Лекция 5.1 Лекция 5.2 Практическое занятие 5 Самостоятельная работа	Традиционная с использованием презентаций, тестирование Выполнение задания Изучение материалов лекций

5 Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: –тестирование (темы 1-5) – практическое задание (темы 1-3) –практическое задание (темы 4-5)	5 баллов 8 баллов 11 баллов	30 баллов 8 баллов 22 баллов
Промежуточная аттестация – зачёт (ответы на вопросы)		40 баллов
Итого за семестр		100 баллов

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	Темы 1 – 5	ПК-10, ПК-4	Опрос
2.	Практические занятия 1 – 5	ПК-10, ПК-4	План практических занятий

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			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	<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 выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	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 выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	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 выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	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 выставляется 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

Примерные контрольные вопросы для зачёта - проверка сформированности компетенций ПК-4, ПК-10

Контрольные вопросы	Реализуемые компетенции
1. Организационная структура системы аттестации ОИ и их функции. Какие ОИ подлежат обязательной аттестации.	ПК-4, ПК-10
2. Федеральные органы по аттестации и их функции.	ПК-4, ПК-10
3. Органы по аттестации объектов и их функции. Задачи и функции органа по аттестации.	ПК-4, ПК-10
4. Деятельность аттестационных комиссий.	ПК-4, ПК-10
5. Проведение экспертиз электронных документов с ЭП/ЭЦП.	ПК-4, ПК-10
6. Продукт Vip Net. Основной функционал.	ПК-4, ПК-10
7. Система ГосСОПКА.	ПК-4, ПК-10
8. Криптографическая защита в ОС Linux.	ПК-4, ПК-10
9. Система SCADA.	ПК-4, ПК-10
10. Стандарт безопасности SCADA IEC-62351.	ПК-4, ПК-10
11. Аудит безопасности в критически важных ИС.	ПК-4, ПК-10
12. Центр управления и оперативного реагирования на инциденты ИБ.	ПК-4, ПК-10
13. Правила безопасности на объектах SCADA.	ПК-4, ПК-10
14. Защита от вредоносного ПО класса STUXNet.	ПК-4, ПК-10
15. Критически важная информационная система. Приказ N 31 ФСТЭК.	ПК-4, ПК-10

Примерные задания для тестирования- проверка сформированности компетенций ПК-4, ПК-10

1. КИИ - это:

- а) критическая информационная инфраструктура
- б) комплексный индикатор излучений.
- в) коэффициент интенсивности излучений.

2. SCADA – это:

- а) сетевое устройство, подключаемое к двум и более сетям.
- б) автоматизированная система управления технологическим производством.
- в) криптошлюз

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники
основные

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

2. *Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»*. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция)* [Электронный ресурс] : Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_220885/, свободный. – Загл. с экрана.
4. *Указ Президента РФ от 30.03.2022 N 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" »*. [Электронный ресурс] : Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_413177/, свободный. – Загл. с экрана.
5. *Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений»* [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127>, свободный. – Загл. с экрана.
6. *Приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»* [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239>, свободный. – Загл. с экрана.
7. *Постановление Правительства Российской Федерации от 17 февраля 2018 г. N 162 «Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»* [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-17-fevralya-2018-g-n-162>, свободный. – Загл. с экрана.
8. *Приказ ФСТЭК России от 6 декабря 2017 г. N 227 «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»* [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227>, свободный. – Загл. с экрана.
9. *Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»* [Электронный ресурс] : Режим доступа : [tps://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31](https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31), свободный. – Загл. с экрана.
10. *Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.* [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3>, свободный. – Загл. с экрана.
11. *Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной*

технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2>, свободный. – Загл. с экрана.

12. Руководящий документ. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-25-iyulya-1997-g>, свободный. – Загл. с экрана.

Литература Основная

1. Корниенко, А. А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры : учебное пособие / А. А. Корниенко, В. С. , А. П. Глухов. — Санкт-Петербург : ПГУПС, 2022. — 63 с. — ISBN 978-5-7641-1837-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/329477>. — Режим доступа: для авториз. пользователей.
2. Пакин, А. И. Информационная безопасность информационных систем управления предприятием : учебное пособие / А. И. Пакин. - Москва : МГАВТ, 2009. - 43 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/401326>. – Режим доступа: по подписке.
3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва: ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1018665>
4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1843022>. – Режим доступа: по подписке..

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Официальный сайт компании Криптопро [Электронный ресурс]: Режим доступа: <http://www.cryptopro.com/>, свободный. – Загл. с экрана.
2. Центр разработки Криптоком [Электронный ресурс]: Режим доступа: <http://www.cryptocom.ru/products/index.html/>, свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
 ELibrary.ru Научная электронная библиотека www.elibrary.ru
 Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

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 обеспечения дисциплины используется материально-техническая база образовательного учреждения:

- 1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. KasperskyEndpointSecurity

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

- 2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Microsoft Share Point 2010
6. Secret Net Studio 8.4
7. Dallas Lock 8.0
8. Vmware Player 15.5 + ГостеваяОСCentOS 7
9. XSpider 7.0
10. Open VPN
11. SoftEther VPN

8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

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

- проверка сформированности компетенций ПК-4, ПК-10

Темы учебной дисциплины предусматривают проведение практических(семинарских) занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения.

Практическое занятие 1(6 ч.). Нормативно-методическая база использования. Краткий обзор руководящих документов - проверка сформированности компетенций ПК-4, ПК-10

Вопросы для обсуждения:

1. Перечень основных нормативно-правовых документов.
2. Современные средства ЗИ промышленных объектов.
3. Понятие SCADA.

Практическое занятие 2(6 ч.). Особенности подходов и методов в области защиты критически важных информационных систем - проверка сформированности компетенций ПК-4, ПК-10

Вопросы для обсуждения:

1. Проведение экспертиз электронных документов с ЭП/ЭЦП.
2. Средства криптографической защиты информации. Основной функционал.
3. Систем ГосСОПКА.

Практическое занятие 3(6 ч.). Аудит и мониторинг систем SCADA - проверка сформированности компетенций ПК-4, ПК-10

Вопросы для обсуждения:

1. Аудит безопасности в критически важных ИС.
2. Центр управления и оперативного реагирования на инциденты ИБ.
3. Правила безопасности на объектах SCADA.

Практическая работа 4 (6 ч.). Проведение анализа информации на предмет целостности - проверка сформированности компетенций ПК-4, ПК-10

Цель работы изучить понятие целостности информации, проанализировать риски информационной безопасности.

Выполнение работы:

1. Составьте таблицу, содержащую причины нарушения целостности информации и мер предосторожности, применяемых для защиты информации на выбранном объекте от потери целостности.
 2. Подготовьте Отчет.
- Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы:

1. Что такое целостность информации?
2. Какие меры можно предпринять для защиты информации?

Практическая работа 5 (8 ч.). Оценка уязвимости информации -проверка сформированности компетенций ПК-4, ПК-10

Цель работы: Ознакомиться с алгоритмами оценки уязвимости информационной безопасности.

Выполнение задание:

1. Загрузите ГОСТ Р ИСО/МЭК то 13335-3-2007 «Методы и средства обеспечения безопасности». Ознакомьтесь с Приложениями С, D и E ГОСТа.
2. Выберите три различных информационных актива организации.
3. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
4. Пользуясь Приложением С ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
5. Пользуясь одним из методов, предложенных в Приложении E ГОСТа, произведите оценку рисков информационной безопасности для Вашего объекта защиты.
6. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

Контрольные вопросы:

Дайте определение понятиям:

1. Уязвимости системы защиты информации
2. Угрозы ИБ
3. Оценка рисков

Дисциплина «Безопасность критически важных информационных систем» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: научить студентов приемам работы с инфраструктурой критически важных информационных систем.

Задачи: формирование у студентов представлений об инфраструктуре критически важных информационных систем, научить студентов использовать механизмы обеспечения юридической значимости документов.

Дисциплина направлена на формирование следующих компетенций:

- ПК-10 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
- ПК-4 -Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций

В результате освоения дисциплины обучающийся должен:

Знать: основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа, нормативные правовые документы в области защиты информации, математические модели безопасности и формальные модели доступа систем, модели и методы защиты операционных систем, основные проектные решения, средства и методы защиты информации от несанкционированного доступа.

Уметь: решать типовые задачи с помощью методов защиты информации от несанкционированного доступа, применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости за счет принятия неправильных эксплуатационных решений; применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия, применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования; уметь применять комплексный подход к обеспечению информационной безопасности объекта КИИ РФ с учетом требований 178 ФЗ и 31 Приказа ФСТЭК.

Владеть: методами разработки и использования защищенных программных средств; навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах; навыками по реализации политик информационной безопасности; навыками обнаружения и устранения неисправности работы, своевременное и оперативное реагирование на внештатные ситуации, умениями настраивать отказоустойчивый кластер с подсистемой “горячего” резервирования

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.