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

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 2026

Безопасность критически важных информационных систем
Рабочая программа дисциплины

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 5 от 25.12.2025

Оглавление

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 технологическихпроектов 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

	ПК-4.2 Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах	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.
	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	Владеть: Навыками обнаружения и устранения неисправности работы, своевременное и оперативное реагирование на внештатные ситуации, умениями настраивать отказоустойчивый кластер с подсистемой “горячего” резервирования

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.

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
5	Лекции	**26**
5	Практические работы	**28**
	Всего:	**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _48_ академических часа.

3 Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Компоненты инфраструктуры**	Основные понятия. Методология. Компоненты

	критически важных информационных систем	инфраструктуры критически важных информационных систем.
2	**Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов**	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. Здесь интересным моментом и отправной точкой дальнейшего моего повествования служит сочетание «совершенствование безопасности функционирования» ИС КВО
3	**Структура современных критически важных информационных систем**	В соответствии с распоряжением Правительства РФ от 23.03.2006 № 411-рс к критически важным относятся совершенно разные по своему предназначению 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. 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 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**.**
4	**Особенности подходов и методов в области защиты критически важных информационных систем**	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.
5	**Использование средств защиты информации**	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». 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. Приказ №31 регламентирует: • Разработку и документирование правил и процедур (политик) обеспечения безопасности; • Требования к защите среды виртуализации; • Обучение и отработку действий пользователей в случае возникновения нештатных (непредвиденных) ситуаций; • Требования по безопасной разработке ПО; • Требования по инцидент-менеджменту и анализу угроз безопасности; • И другие факторы, обеспечивающие должный уровень безопасности объектов. 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. В автоматизированной системе управления объектами защиты являются: • 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 электронной подписи для придания юридической значимости электронных документов	Лекция 2 Практическое занятие 2. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания 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*

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.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
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

Примерные контрольные вопросы для зачёта

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

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. Методический документ ФСТЭК России от 11 ноября 2025 г. «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-noyabrya-2025-g, свободный. – Загл. с экрана.
7. Приказ Федеральной службы безопасности Российской Федерации от 23.12.2025 № 539 "Об утверждении Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения" [Электронный ресурс] : Режим доступа : http://publication.pravo.gov.ru/document/0001202512260014
8. Приказ ФСБ России от 26 декабря 2025 г. № 554 “Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе к средствам, предназначенным для поиска признаков компьютерных атак” [Электронный ресурс] : Режим доступа : https://www.garant.ru/products/ipo/prime/doc/413295790/
9. Приказ ФСТЭК России от 11.04.2025 № 117 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений"
10. Приказ ФСТЭК России от 20 апреля 2023 г. № 69 «О внесении изменений в требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. N 235» [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-20-aprelya-2023-g-n-69, свободный. – Загл. с экрана.
11. Приказ ФСТЭК России от 28 мая 2020 г. № 75 «Об утверждении порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования». [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-28-maya-2020-g-n-75, свободный. – Загл. с экрана.
12. Приказ ФСТЭК России от 25 декабря 2017 г. № 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.
13. Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] : Режим доступа : ttps://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-17-fevralya-2018-g-n-162, свободный. – Загл. с экрана.
14. 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.

15. Приказ ФСТЭК России от 14 марта 2014 г. № 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, свободный. – Загл. с экрана.
16. 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.
17. 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.
18. 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. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628. – Режим доступа: по подписке.
3. 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..

Дополнительная

4. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов,

М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 25.02.2026). – Режим доступа: по подписке.

5. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 602 с. — (Высшее образование: Специалитет). — DOI 10.12737/2143785. - ISBN 978-5-16-019905-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2143785. – Режим доступа: по подписке.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Официальный сайт компании Криптопро: http://www.cryptopro.com/
Центр разработки Криптоком: http://www.cryptocom.ru/products/index.html/

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ruwww.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 + ГостеваяОССentOS 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 использова-

нием 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

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

Вопросы для обсуждения:

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

Практическое занятие 2(6 ч.). Особенности подходов и методов в области защиты критически важных информационных систем

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

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

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

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 Е 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 Е 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

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

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.

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