**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
*Направление подготовки 10.03.01 Информационная безопасность*
*Направленность (профиль) подготовки*
*Безопасность автоматизированных систем*
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

*Безопасность критически важных информационных систем*
*Рабочая программа дисциплины*
*Составитель:*
*Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков*

*Ответственный редактор*
*Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин*

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

**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** |
|---|---|---|
| *ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности* | *ОПК-5.1 Знает основы законодательства Российской Федерации, нормативные правовоые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации* | *Знать: основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа, нормативные правовые документы в области защиты информации, основные проектные решения, средства и методы защиты информации от несанкционированного доступа.* |
| | *ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав* | *Уметь: решать типовые задачи с помощью методов защиты информации от несанкционированного доступа, применять современные методы и методики защиты авторских прав на IT-продукцию (изделие) от несанкционированного исследования, копирования, распространения и использования.* |

| | | |
|---|---|---|
| | *ОПК-5.3*<br>*Владеет навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации* | *Владеть:*<br>*навыками разработки методических документов и ОРД, технических регламентов в области ИБ.* |
| *ПК-10*<br>*Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности* | *ПК-10.1*<br>*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*<br>*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*<br>*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*<br>*Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций* | *ПК-4.1*<br>*Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем* | *Знать:*<br>*методы и способы обеспечения отказоустойчивости АС, основы администрирования защищенных АС и подсистем безопасности объектов КИИ РФ* |

| | | |
|---|---|---|
| | *ПК-4.2*<br>*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*<br>*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:*<br>*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 факультативным дисциплинам по выбору части, формируемой участниками образовательных отношений блока дисциплин учебного плана.
Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: "Безопасность операционных систем", "Оценка безопасности программного обеспечения автоматизированных систем".
В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: "Защита информации от вредоносного программного обеспечения", "Безопасность программного обеспечения автоматизированных систем", "Информационная безопасность телекоммуникационных систем".

## 2. Структура дисциплины

### Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 40 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** | *Компоненты инфраструктуры критически важных информационных систем* | **2** | **2** | | **4** | | | **4** | Опрос. Оценка выполнения практических заданий |
| **2** | *Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов* | **2** | **2** | | **4** | | | **8** | Опрос. Оценка выполнения практических заданий |
| **3** | *Структура современных критически важных информационных систем* | **2** | **4** | | **6** | | | **8** | Опрос. Оценка выполнения практических заданий |
| **4** | *Особенности подходов и методов в области защиты критически важных информационных систем* | **2** | **4** | | **4** | | | **8** | Опрос. Оценка выполнения практических заданий |
| **5** | *Использование средств защиты информации* | **2** | **4** | | **4** | | | **8** | Оценка выполнения практических заданий |
| | *Зачёт* | | | | **2** | | | | *Зачёт по билетам* |
| | итого: | | **16** | | **24** | | | **36** | |

**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** | 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.<br><br>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.<br>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».<br>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.<br>Приказ №31 регламентирует:<br>• Разработку и документирование правил и процедур (политик) обеспечения безопасности;<br>• Требования к защите среды виртуализации;<br>• Обучение и отработку действий пользователей в случае возникновения нештатных (непредвиденных) ситуаций;<br>• Требования по безопасной разработке ПО; |

| | | |
|---|---|---|
| | | • Требования по инцидент-менеджменту и анализу угроз безопасности;<br>• И другие факторы, обеспечивающие должный уровень безопасности объектов.<br>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.<br>В автоматизированной системе управления объектами защиты являются:<br>• Информация о параметрах (состоянии) управляемого объекта или процесса, управляющая информация, контрольно-измерительная информация, иная критически важная (технологическая) информация;<br>• 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*<br><br>*Практическое занятие 1.*<br><br>*Самостоятельная работа* | *Традиционная с использованием презентаций*<br>*Выполнение задания*<br><br>*Изучение материалов лекций* |
| *2* | *Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов* | *Лекция 2*<br><br>*Практическое занятие 2.*<br><br>*Самостоятельная работа* | *Традиционная с использованием презентаций*<br>*Выполнение задания*<br><br>*Изучение материалов лекций* |

| | | | |
|---|---|---|---|
| *3* | *Структура современных критически важных информационных систем* | *Лекция 3.1*<br>*Лекция 3.2*<br><br>*Практическое занятие 3.*<br><br>*Самостоятельная работа* | *Традиционная с использованием презентаций*<br><br>*Выполнение задания*<br><br>*Изучение материалов лекций* |
| *4* | *Функции удостоверяющего центра* | *Лекция 4.1*<br>*Лекция 4.2*<br><br>*Практическое занятие 4*<br><br>*Самостоятельная работа* | *Традиционная с использованием презентаций*<br><br>*Выполнение задания*<br><br>*Изучение материалов лекций* |
| *5* | *Использование функций провайдера криптографических услуг* | *Лекция 5.1*<br>*Лекция 5.2*<br><br>*Практическое занятие 5*<br><br>*Самостоятельная работа* | *Традиционная с использованием презентаций*<br><br>*Выполнение задания*<br><br>*Изучение материалов лекций* |

**5. Оценка планируемых результатов обучения**

5.1. Система оценивания

| **Форма контроля** | **Макс. количество баллов** | |
|---|---|---|
| | **За одну работу** | **Всего** |
| Текущий контроль:<br>*– опрос (темы 1-5)*<br>*– практическое задание (темы 1-3)*<br>*– практическое задание (темы 4-5)* | <br>*5 баллов*<br>*6 баллов*<br>*7 баллов* | <br>*30 баллов*<br>*6 баллов*<br>*14 баллов* |
| Промежуточная аттестация<br>*зачёт* | | *40 баллов* |
| **Итого за дисциплину**<br>*зачёт* | | *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 | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 | Опрос |
| 2. | Практические занятия 1 – 5 | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1, | 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:

<table>
<tr><td>100-балльная шкала</td><td colspan="2">Традиционная шкала</td><td>Шкала ECTS</td></tr>
<tr><td>95 – 100</td><td rowspan="2">отлично</td><td rowspan="5">зачтено</td><td>A</td></tr>
<tr><td>83 – 94</td><td>B</td></tr>
<tr><td>68 – 82</td><td>хорошо</td><td>C</td></tr>
<tr><td>56 – 67</td><td rowspan="2">удовлетворительно</td><td>D</td></tr>
<tr><td>50 – 55</td><td>E</td></tr>
<tr><td>20 – 49</td><td rowspan="2">неудовлетворительно</td><td rowspan="2">не зачтено</td><td>FX</td></tr>
<tr><td>0 – 19</td><td>F</td></tr>
</table>

5.2.Критерии выставления оценки по дисциплине

| **Баллы/ Шкала ECTS** | **Оценка по дисциплине** | **Критерии оценки результатов обучения по дисциплине** |
|---|---|---|
| 100-83/ A,B | «отлично»/ «зачтено (отлично)»/ «зачтено» | Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.<br>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.<br>Свободно ориентируется в учебной и профессиональной литературе.<br><br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий». |
| 82-68/ C | «хорошо»/ «зачтено (хорошо)»/ «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.<br>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.<br>Достаточно хорошо ориентируется в учебной и профессиональной литературе.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.<br>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший». |
| 67-50/ D,E | «удовлетворительно»/ «зачтено (удовлетворительно)»/ «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.<br>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.<br>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.<br>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. |

| Баллы/ Шкала ECTS | Оценка по дисциплине | Критерии оценки результатов обучения по дисциплине |
|---|---|---|
| | | Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный». |
| 49-0/ F,FX | «неудовлетворительно»/ 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[1]

Примерные контрольные вопросы для зачёта - проверка сформированности компетенций ПК-4,ПК-10, ОПК-5

| Контрольные вопросы | Реализуемые компетенции |
|---|---|
| 1. Организационная структура системы аттестации ОИ и их функции. Какие ОИ подлежат обязательной аттестации. | ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 2. Федеральные органы по аттестации и их функции. | ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 3. Органы по аттестации объектов и их функции. Задачи и функции органа по аттестации. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 4. Деятельность аттестационных комиссий. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 5. Проведение экспертиз электронных документов с ЭП/ЭЦП. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |

[1] Приводятся примеры оценочных средств в соответствии со структурой дисциплины и системой контроля: варианты тестов, тематика письменных работ, примеры экзаменационных билетов, типовые задачи, кейсы и т.п. Оценочными средства должны быть обеспечены все формы текущего контроля и промежуточной аттестации. Они должны быть ориентированы не только на проверку сформированности знаний, но также умений и владений.

| | |
|---|---|
| 6. Продукт Vip Net. Основной функционал. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 7. Система ГосСОПКА. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 8. Криптографическая защита в ОС Linux. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 9. Система SCADA. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-4.3, ПК-4.2, ПК- 4.1 |
| 10. Стандарт безопасности SCADA IEC-62351. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 11. Аудит безопасности в критически важных ИС. | ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 12. Центр управления и оперативного реагирования на инциденты ИБ. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 13. Правила безопасности на объектах SCADA. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 14. Защита от вредоносного ПО класса STUXNet. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |
| 15. Критически важная информационная система. Приказ N 31 ФСТЭК. | ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-10.3, ПК-10.2, ПК-10.1, ПК-4.3, ПК-4.2, ПК- 4.1 |

***Примерные задания для тестирования- проверка сформированности компетенций ПК-4,ПК-10, ОПК-5***

**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 прозводством.*
в) криптошлюз

## 6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники
основные

1. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа :

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.

2. *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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
3. *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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
4. *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/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

## Литература
### Основная

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450371
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
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. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт,

2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430

5. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063
6. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
7. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107
8. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 Информационная безопасность : по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О. В. ; отв. ред. А. А. Тарасов]. - Электрон. дан. - Москва: РГГУ, 2013. - 30 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009341. - Загл. с экрана. - ISBN 978-5-7281-1789-6.

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.

## 7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

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

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

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

| №п /п | Наименование ПО | Производитель | Способ распространения (лицензионное или свободно распространяемое) |
|---|---|---|---|
| 1 | Microsoft Office 2010 | Microsoft | лицензионное |
| 2 | Windows 7 Pro | Microsoft | лицензионное |
| 3 | Microsoft Share Point 2010 | Microsoft | лицензионное |
| 4 | Microsoft Office 2013 | Microsoft | лицензионное |
| 5 | Windows 10 Pro | Microsoft | лицензионное |

| | | | |
|---|---|---|---|
| 6 | Kaspersky Endpoint Security | Kaspersky | Лицензионное |
| 7 | Secret Net Studio 8.4 | Код безопасности | Режим доступа: https://securitycode.ru Демо-версия |
| 8 | Dallas Lock 8.0 | Конфидент | Режим доступа: https://dallaslock.ru/ Демо-версия |
| 9 | Vmware Player 15.5 + Гостевая ОС CentOS 7 | VMWare | Режим доступа: https://www.vmware.com/products/ Демо-версия<br><br>Открытое ПО Режим доступа: https://www.centos.org/download/ Инсталляционный дистрибутив Linux |
| 10 | XSpider 7.0 | Positive Technologies | Режим доступа: https://www.ptsecurity.com/ru-ru/ Демо-версия |
| 11 | Open VPN | OpenVPN | Свободное ПО, Режим доступа: https://openvpn.net/ |
| 12 | SoftEther VPN | SoftEther | Свободное ПО, Режим доступа: https://www.softether.org/ |

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

**Перечень БД и ИСС**

| №п/п | Наименование |
|---|---|
| 1 | Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г.<br>Web of Science<br>Scopus |
| 2 | Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г.<br>Журналы Cambridge University Press<br>ProQuest Dissertation & Theses Global<br>SAGE Journals<br>Журналы Taylor and Francis |
| 3 | Профессиональные полнотекстовые БД |

| | |
|---|---|
| | JSTOR<br>Издания по общественным и гуманитарным наукам<br>Электронная библиотека Grebennikon.ru |
| 4 | Компьютерные справочные правовые системы<br>Консультант Плюс,<br>Гарант |

## 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, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

**9. Методические материалы[2]**

9.1. Планы практических занятий - проверка сформированности компетенций ПК-4,ПК-10, ОПК-5

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(4 ч.).Нормативно-методическая база использования. Краткий обзор руководящих документов** - проверка сформированности компетенций ПК-4,ПК-10, ОПК-5

*Вопросы для обсуждения*:

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

Список литературы:

Приведён в п. 6 данной РПД

*Материально-техническое обеспечение занятия*: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, VPN-клиент.

---

[2] Методические материалы по дисциплине могут входить в состав рабочей программы, либо разрабатываться отдельным документом.

**Практическое занятие 2(4 ч.). Особенности подходов и методов в области защиты критически важных информационных систем** - проверка сформированности компетенций ПК-4,ПК-10, ОПК-5

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

Список литературы:
Приведён в п. 6 данной РПД

*Материально-техническое обеспечение занятия*: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, VPN-клиент.

**Практическое занятие 3(6 ч.). Аудит и мониторинг систем SCADA** - проверка сформированности компетенций ПК-4,ПК-10, ОПК-5

**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.

Список литературы:
Приведён в п. 6 данной РПД

*Материально-техническое обеспечение занятия*: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, VPN-клиент, сканер уязвимостей (XSpider).

**Практическая работа 4 (4 ч.). Проведение анализа информации на предмет целостности -** проверка сформированности компетенций ПК-4,ПК-10, ОПК-5

**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?

Список литературы:
Приведён в п. 6 данной РПД

*Материально-техническое обеспечение занятия*: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer.

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

**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 C, 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 C 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

Список литературы:
Приведён в п. 6 данной РПД

*Материально-техническое обеспечение занятия*: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer

*Приложение 1*

## АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Безопасность критически важных информационных систем» реализуется на факультете Информационных систем и безопасности для студентов 1-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – Безопасность автоматизированных систем) 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:

- ОПК-5.1 - Знает основы законодательства Российской Федерации, нормативные правовоые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации
- ОПК-5.2 -Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав
- ОПК-5.3 -Владеет навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации
- 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
- 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
- ПК-10.3 -Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации
- 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

- ПК-4.2 -Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах

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

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 2 зачётные единицы.

*Приложение 2*

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

**ЛИСТ ИЗМЕНЕНИЙ**

в рабочей программе дисциплины Безопасность критически важных информационных систем
*(название дисциплины)*
по направлению подготовки Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
*(элемент рабочей программы)*
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
*(элемент рабочей программы)*
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
*(элемент рабочей программы)*
3.1. ……..;
3.2. ……...;
…
3.9. …… .

*Составитель подпись расшифровка подписи*
*дата*