

**МИНОБРНАУКИ РОССИИ**

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

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

**ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ, УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
*Направление подготовки 10.03.01 Информационная безопасность*  
*Направленность (профиль) подготовки*  
*№ 2 Организация и технология защиты информации*  
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2017

*Инфраструктура открытых ключей, удостоверяющие центры*

*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

№ 6 от 24.01.2017 г. \_\_\_\_\_

## **ОГЛАВЛЕНИЕ**

### **1. Пояснительная записка**

#### 1.1 Цель и задачи дисциплины

#### 1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

#### 1.3. Место дисциплины в структуре образовательной программы

### **2. Структура дисциплины**

### **3. Содержание дисциплины**

### **4. Образовательные технологии**

### **5. Оценка планируемых результатов обучения**

#### 5.1. Система оценивания

#### 5.2. Критерии выставления оценок

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

### **6. Учебно-методическое и информационное обеспечение дисциплины**

#### 6.1. Список источников и литературы

#### 6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

### **7. Материально-техническое обеспечение дисциплины**

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

### **9. Методические материалы**

#### 9.1. Планы лабораторных занятий

## **Приложения**

### Приложение 1. Аннотация дисциплины

### Приложение 2. Лист изменений

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

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

Задачи: изучение инфраструктуры открытых ключей, освоение принципов формирования электронной подписи, выработка умений настройки компонентов инфраструктуры.

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

<i><b>Коды компетенции</b></i>	<i><b>Содержание компетенций</b></i>	<i><b>Перечень планируемых результатов обучения по дисциплине</b></i>
<i><b>ПК-1</b></i>	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать: архитектуру и компоненты инфраструктуры открытых ключей; юридические и методические основы обеспечения юридической значимости электронных документов; принципы формирования электронной подписи; формат цифрового сертификата. Уметь: пользоваться основными крипто провайдерами, в части формирования электронной подписи; разворачивать такие компоненты инфраструктуры как удостоверяющие центры; выбирать, устанавливать и настраивать компоненты инфраструктуры, принимать участие в разработке политики безопасности. Владеть: профессиональной терминологией; навыками настройки и эксплуатации компонентов инфраструктуры открытых ключей.

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Инфраструктура открытых ключей, удостоверяющие центры» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: "Безопасность операционных систем", "Математические основы защиты информации", "Вычислительные сети".

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: "Администрирования подсистем защиты информации", "Безопасность программного обеспечения", "Аттестация объектов информатизации".

## 2. Структура дисциплины

### Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 44 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятель- ная работа	Формы текущего контроля успева- емости, форма промежу- точной аттеста- ции (по семест- рам)
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточ- ная аттестация		
1	Компоненты инфра- структуры откры- тых ключей	6	2					10	Опрос
2	Нормативно- методическая база использования элек- тронной подписи для придания юридиче- ской значимости электронных доку- ментов	6	2					10	Опрос. Защита лабора- торных работ.
3	Структура цифро- вых сертификатов	6	4		4			6	Опрос. Защита лабора- торных работ.
4	Функции удостове- ряющего центра	6	4		4			4	Опрос. Защита лабора- торных работ.
5	Использование функ- ций провайдера криптографических услуг	6	4		4			14	Опрос. Защита лабора- торных работ.
	зачёт								Зачёт по билетам
	итоги:		16		12			44	

### 3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Компоненты инфраструктуры открытых ключей	PKI реализуется в модели клиент-сервер, то есть проверка какой-либо информации, предоставляемой инфраструктурой, может происходить только по инициативе клиента. Основные компоненты PKI: Удостоверяющий центр (УЦ) является основной структурой, формирующей цифровые сертификаты подчиненных центров сертификации и конечных пользователей. УЦ является главным

		<p>компонентом PKI: он является доверенной третьей стороной (trusted third party) это сервер, который осуществляет управление жизненным циклом сертификатов (но не их непосредственным использованием).</p>
2	<b>Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов</b>	<p>Сертификат открытого ключа (чаще всего просто сертификат) — это данные пользователя и его открытый ключ, скреплённые электронной подписью удостоверяющего центра. Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет закрытым ключом, который соответствует этому открытому ключу.</p> <p>Репозиторий — хранилище, содержащее сертификаты и списки отозванных сертификатов (СОС) и служащее для распространения этих объектов среди пользователей. В Федеральном Законе РФ № 63 «Об электронной подписи» он называется реестр сертификатов ключей подписей.</p>
3	<b>Структура цифровых сертификатов</b>	<p>Структура сертификата</p> <ul style="list-style-type: none"> <li>• Версия</li> <li>• Серийный номер</li> <li>• Идентификатор алгоритма подписи</li> <li>• Имя издателя</li> <li>• Период действия</li> <li>• Имя субъекта</li> <li>• Информация об открытом ключе субъекта:</li> <li>• Алгоритм открытого ключа</li> <li>• Открытый ключ субъекта</li> <li>• Уникальный идентификатор издателя (обязательно только для v2 и v3)</li> <li>• Уникальный идентификатор субъекта (обязательно только для v2 и v3)</li> <li>• Дополнения (для v2 и v3)</li> <li>• Возможные дополнительные детали</li> <li>• Алгоритм подписи сертификата (обязательно только для v3)</li> <li>• Подпись сертификата (обязательно для всех версий)</li> </ul>
4	<b>Функции удостоверяющего центра</b>	<p>Регистрационный центр (РЦ) — необязательный компонент системы, предназначенный для регистрации пользователей. Для этих целей РЦ обычно предоставляет веб-интерфейс. Удостоверяющий центр доверяет регистрационному центру проверку информации о субъекте. Регистрационный центр, проверив правильность инфор-</p>

		мации, подписывает её своим ключом и передаёт удостоверяющему центру, который, проверив ключ регистрационного центра, выписывает сертификат. Один регистрационный центр может работать с несколькими удостоверяющими центрами (то есть состоять в нескольких РКІ), один удостоверяющий центр может работать с несколькими регистрационными центрами. Иногда, удостоверяющий центр выполняет функции регистрационного центра.
5	<b>Использование функций провайдера криптографических услуг</b>	<p>Архив сертификатов — хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком действия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы.</p> <p>Центр запросов — необязательный компонент системы, где конечные пользователи могут запросить или отозвать сертификат.</p> <p>Конечные пользователи — пользователи, приложения или системы, являющиеся владельцами сертификата и использующие инфраструктуру управления открытыми ключами.</p>

#### 4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Компоненты инфраструктуры открытых ключей	<p>Лекция 1.</p> <p>Самостоятельная работа</p>	<p>Традиционная с использованием презентаций</p> <p>Изучение материалов лекций</p>
2	Нормативно-методическая база использования электронной подписи для придания юридической значимости электронным документам	<p>Лекция 2.</p> <p>Самостоятельная работа</p>	<p>Традиционная с использованием презентаций</p> <p>Изучение материалов лекций</p>
3	Структура цифровых сертификатов	<p>Лекция 3.1</p> <p>Лекция 3.2</p> <p>Практическое занятие 1.</p> <p>Самостоятельная работа</p>	<p>Традиционная с использованием презентаций</p> <p>Выполнение задания</p> <p>Изучение материалов лекций</p>
4	Функции удостоверяющего центра	<p>Лекция 4.1</p> <p>Лекция 4.2</p>	<p>Традиционная с использованием презентаций</p> <p>Выполнение задания</p>

		<i>Практическое занятие 2.</i> <i>Самостоятельная работа</i>	<i>Изучение материалов лекций</i>
5	<i>Использование функций провайдера криптографических услуг</i>	<i>Лекция 5.1</i> <i>Лекция 5.2</i>  <i>Практическое занятие 3.</i> <i>Самостоятельная работа</i>	<i>Традиционная с использованием презентаций</i>  <i>Выполнение задания</i> <i>Изучение материалов лекций</i>

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: – опрос (темы 1-5) – лабораторное задание (темы 3) – лабораторное задание (темы 4-5)	5 баллов 6 баллов 7 баллов	30 баллов 6 баллов 14 баллов
Промежуточная аттестация зачёт		40 баллов
<b>Итого за дисциплину</b> зачёт		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	«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. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности,

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. 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».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «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. 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».</p>
49-0/ F,FX	«неудовлетворительно»/ 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. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходи-</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>мыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

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

Примерные контрольные вопросы для зачёта - проверка сформированности компетенций ПК-1

1. Организационная структура системы аттестации ОИ и их функции. Какие ОИ подлежат обязательной аттестации.
2. Федеральные органы по аттестации и их функции.
3. Органы по аттестации объектов и их функции. Задачи и функции органа по аттестации.
4. Деятельность аттестационных комиссий.
5. Сертификация открытого ключа.
6. Логическая структура и компоненты РКІ.
7. Риски использования ЭЦП.
8. Заявители и их функции. Заявка на проведение аттестации ОИ.
9. Порядок проведения аттестации объектов информатизации. Содержание заявок.
10. Порядок взаимодействия заявителя и органа по проведению аттестации.
11. Проведение экспертиз электронных документов с ЭП/ЭЦП.
12. Организационно-штатное обеспечение деятельности УЦ.
13. Основные понятия технологии РКІ.
14. Функции удостоверяющего центра.
15. Процедура оформления заявок на получения сертификата в УЦ.
16. Структура цифрового сертификата формата X.509 v.3
17. Заключительный этап аттестации ОИ. Условия получения аттестата соответствия.
18. Что должно содержать заключение аттестационной комиссии.
19. Списки отозванных сертификатов.
20. Эксплуатация аттестованного объекта.
21. Рассмотрение апелляций по вопросам аттестации УЦ.
22. Интерфейс ОС Windows для работы с сертификатами.
23. Применение ЭП для обеспечения юридической значимости электронных документов.
24. Процедуры формирования и проверки ЭП.
25. Носители ключевой информации.
26. Функции криптопровайдера Криптопро-CSP
27. Аттестационные испытания ВП. Что входит в проверку систем ЗИ.
28. Интеграция функций криптопровайдера в офисные пакеты.
29. Использование УЦ.
30. Виды ЭЦП.
31. Основные разработчики пакетов для работы с РКІ.
32. Перечень основных разработчиков CSP.
33. Требования к шифрованию при работе с государственными Заказчиками.

34. Компроментация ключей.
35. Продукт Vip Net. Основной функционал.
36. Продукт OpenVPN. Основной функционал.
37. Криптографическая защита в ОС Linux.
38. Квантовая криптография. Пути развития.
39. УЦ. Исследование уязвимостей.
40. Утилиты для работы с SSL в Linux.
41. Работа с корневыми сертификатами.
42. Аудит безопасности в УЦ.
43. Расследование инцидентов при краже ключей УЦ.
44. Административная ответственность за нарушение регламента работы УЦ.
45. Центр управления сетью в VIP Net.
46. Правила безопасности Iptables.
47. Конфигурирование сервиса Fail2ban.
48. Взаимодействие компонентов инфраструктуры открытых ключей.

**Примерные задания для тестирования- проверка сформированности компетенций ПК-1**

**1. Что такое iptables:**

- а) консоль управления МЭ netfilter.
- б) полноценный фаерволл.
- в) сетевой мост.

**2. Fail2ban – это:**

- а) Медиа-проигрыватель.
- б) Утилита для блокирования несанкционированного доступа.
- в) Сервер приложений.

**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/](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/](http://www.consultant.ru/document/cons_doc_LAW_61801/), свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» [Электронный ресурс]: Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_112701/](http://www.consultant.ru/document/cons_doc_LAW_112701/), свободный. – Загл. с экрана.
4. *Федеральный закон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» [Электронный ресурс]: Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_40241/](http://www.consultant.ru/document/cons_doc_LAW_40241/), свободный. – Загл. с экрана.

**Литература**

**Основная**

1. *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>

2. *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>

#### 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.

#### 6.3. Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

### 7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:

- лицензионное ПО MS Windows 7 и старше;
- лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше

2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлены:

- лицензионное ПО MS Windows 7 и старше;
- лицензионное ПО MS Office 2010 и старше;
- программный гипервизор VMware Player;
- программа CryptoPro

#### Перечень 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	VMware Player 15.5 +	VMWare	Свободное ПО, Режим доступа:

	Гостевая ОС CentOS 7		<a href="https://www.vmware.com/products/">https://www.vmware.com/products/</a> Демо-версия  Открытое ПО Режим доступа: <a href="https://www.centos.org/download/">https://www.centos.org/download/</a> Инсталляционный дистрибутив Linux
8	демо-дистрибутивы СКЗИ «Крипто-Про».	Крипто-Про	Свободное ПО, Режим доступа: <a href="https://www.cryptopro.ru/user?destination=node%2F148">https://www.cryptopro.ru/user?destination=node%2F148</a>  Демо-версия

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

## **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 работ. Методические указания по организации и проведению**

Темы учебной дисциплины предусматривают проведение практических работ, 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. Помощь в этом оказывают задания для практических работ, выдаваемые преподавателем на

каждом занятии, задания на самостоятельную подготовку, перечень вопросов для подготовки к зачету и контрольные домашние задания для самостоятельной работы студентов.

**Целью** практических работ является закрепление теоретического материала и приобретение практических навыков использования методов применения пакетов компьютерной математики в профессиональной деятельности, применять навыки для принятия наиболее эффективных решений в условиях быстро меняющейся реальности, для быстрой адаптации к изменяющимся условиям деятельности.

Тематика практических работ соответствует программе курса.

1. Работа с сертификатами в ОС Windows.
2. Функции удостоверяющего центра на примере тестового УЦ Криптопро.
3. Настройки криптопровайдера Криптопро CSP.
4. Функции криптобиблиотеки OpenSSL.

Методические указания к практическим работам приведены в отдельном документе.

## **9.2. Методические указания для обучающихся по освоению дисциплины**

Успешное освоение дисциплины студентом определяется, несколькими факторами: посещение аудиторных занятий, подготовка и выполнение домашних заданий, своевременное выполнение запланированных форм отчетности.

Самостоятельная работа студентов направлена на закрепление полученных навыков и для приобретения новых теоретических и фактических знаний, выполняется в читальном зале библиотеки и в домашних условиях, подкрепляется учебно-методическим и информационным обеспечением (учебники, учебно-методические пособия, конспекты лекций).

Самостоятельная работа выполняется студентами с использованием ПК в домашних условиях, либо в библиотеке института по специальным заданиям в соответствии с методическими материалами, выданными преподавателем. Самостоятельная работа включает отработку навыков анализа ситуации, создание модели ситуации, которая используется в данном конкретном методе выбора наилучшей альтернативы, и решение задачи, также к самостоятельной работе относится подготовка к практическим работам, подготовка по темам пропущенных занятий.

Начиная с первого занятия, преподаватель объявляет студентам тему следующего занятия и список литературы. Студент должен ознакомиться с предложенными источниками, в таком случае он на следующем занятии будет готов к восприятию нового материала.

Студент для самостоятельной работы должен иметь программу курса, вопросы к зачету, список основной и дополнительной литературы по курсу.

После каждого занятия, перед следующим, студент должен ознакомиться с пройденным материалом. При возникновении вопросов или непонимания, студент должен изучить рекомендованную и дополнительную литературу по курсу.

**АННОТАЦИЯ ДИСЦИПЛИНЫ**

Дисциплина «Инфраструктура открытых ключей, удостоверяющие центры» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации) кафедрой комплексной защиты информации.

Цель дисциплины: научить студентов приемам работы с инфраструктурой открытых ключей и цифровыми сертификатами.

Задачи: формирование у студентов представлений об инфраструктуре открытых ключей, выработка умений разворачивать и настраивать удостоверяющие центры, научить студентов использовать механизмы обеспечения юридической значимости документов.

Дисциплина направлена на формирование следующих компетенций:

- ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

В результате освоения дисциплины обучающийся должен:

Знать архитектуру и компоненты инфраструктуры открытых ключей;

юридические и методические основы обеспечения юридической значимости электронных документов; принципы формирования электронной подписи;

формат цифрового сертификата.

Уметь пользоваться основными крипто провайдерами, в части формирования электронной подписи; разворачивать такие компоненты инфраструктуры как удостоверяющие центры; выбирать, устанавливать и настраивать компоненты инфраструктуры, принимать участие в разработке политики безопасности.

Владеть профессиональной терминологией; навыками настройки и эксплуатации компонентов инфраструктуры открытых ключей.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

## ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.06.2017	<b>10</b>
2	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2018 г.)</i>	26.06.2018	<b>11</b>
3	Обновлен раздел 9. Методические материалы	26.06.2018	<b>11</b>
4	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	26.06.2018	<b>11</b>
5	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.08.2019	<b>1</b>
6	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)</i>	23.06.2020	<b>14</b>
7	Обновлена основная и дополнительная литература	23.06.2020	<b>14</b>
8	Обновлен раздел п.4 Образовательные технологии	23.06.2020	<b>14</b>
9	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	23.06.2020	<b>14</b>

**1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2017 г.)****Перечень ПО***Таблица 1*

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

**Перечень БД и ИСС***Таблица 2*

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

**2. Обновление структуры дисциплины (модуля) для очной формы обучения (2018 г.)****Структура дисциплины (модуля) для очной формы обучения**

Общая трудоёмкость дисциплины составляет 2 з.е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 44 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 открытых ключей	6	2						10	Опрос
2	Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов	6	2						10	Опрос. Защита лабораторных работ.
3	Структура цифровых сертификатов	6	4			4			6	Опрос. Защита лабораторных работ.
4	Функции удостоверяющего центра	6	4			4			4	Опрос. Защита лабораторных работ.
5	Использование функций провайдера криптографических услуг	6	4			4			14	Опрос. Защита лабораторных работ.
	зачёт									Зачёт по билетам
	итоги:		16			12			44	

**3. Обновление раздела 9. Методические материалы**

В раздел 9 внести следующие изменения.

1. Заменить производные слова от слова «практический» на соответствующие производные слова от слова «лабораторный».

Внести изменения в подраздел **9.1. Планы лабораторных занятий** - проверка сформированности компетенций ПК-1

Темы учебной дисциплины предусматривают проведение лабораторных 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.

Лабораторные занятия проводятся в учебных группах (подгруппах) и имеют своей целью:

- 1) закрепление теоретических основ дисциплины, излагаемых в лекционном курсе, а также самостоятельно изучаемых студентами;
- 2) формирование практических навыков по использованию по моделированию системы охраны объектов;
- 3) научить студентов использовать экспериментальные и научные исследования в производственной деятельности по созданию, сопровождению и эксплуатации систем охраны объектов от физического доступа посторонних лиц.

**Лабораторное занятие 1(4 ч.). Исследование механизмов защиты ЭЦП** (проверка сформированности компетенций ПК-1)

*Цель работы:* получение практических навыков в исследовании ЭЦП.

*Указания по выполнению задания:* обратить внимание на длину ключей при работе с ЭЦП.

*Выполнение задания:*

В ходе практической работы имитируется процесс, осуществляющий несанкционированный доступ к ресурсам ОС. Задача студентам, как будущим администраторам СЗИ, своевременно анализировать и выявлять подобные угрозы.

*Контрольные вопросы:*

1. Виды сертификатов.
2. Методы компрометации ключей.
3. Методы демаскирования вредоносных программных агентов при работе с ЭЦП.

Список литературы:

Приведён в п. 6 данной РПД

*Материально-техническое обеспечение практического занятия:* аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

**Лабораторное занятие 2(4 ч.). Структура цифровых сертификатов. Ознакомления студентов с обязательными и дополнительными полями сертификатов** (проверка сформированности компетенций ПК-1)

*Цель работы:* получение практических навыков работы с сертификатами.

*Указания по выполнению задания:* обратить внимание на дополнительные поля сертификата.

*Выполнение задания:*

В ходе практической работы студенты обучаются создавать сертификаты и их импортирования в УЦ.

*Контрольные вопросы:*

1. Структура сертификата
2. Процедура отзыва сертификата в УЦ.
3. Процедура импортирования сертификатов.

Список литературы:

Приведён в п. 6 данной РПД

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

гостевой ОС VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

**Лабораторное занятие 3(2 ч.).Использование функций провайдера криптографических услуг. Приобретение студентами навыков работы с утилитами СКЗИ «Крипто-Про»** (проверка сформированности компетенций ПК-1)

*Цель работы:* получение практических навыков работы с СКЗИ «Крипто-Про».

*Указания по выполнению задания:* обратить внимание на использование плагина при работе с графической оболочкой в Web-браузере.

*Выполнение задания:*

В ходе практической работы студенты обучаются с продуктами СКЗИ «Крипто-Про»..

*Контрольные вопросы:*

1.Назначение СКЗИ «Крипто-Про»..

2.Перечень алгоритмов шифрования, поддерживаемых СКЗИ «Крипто-Про»..

3. Поддержка плагина СКЗИ «Крипто-Про» разными браузерами.

Список литературы:

Приведён в п. 6 данной РПД

*Материально-техническое обеспечение практического занятия:* аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС VMPlayer с гостевой ОС CentOS 7, демо-дистрибутивы СКЗИ «Крипто-Про». Занятия проводятся в специально оборудованном компьютерном классе.

**4. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)**

**Перечень ПО**

Таблица 1

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

**Перечень БД и ИСС**

Таблица 2

№п/п	Наименование
------	--------------

	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

К.т.н., доцент, А.С. Моляков

**5.Обновление состава программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)**  
**Перечень ПО**

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

**Перечень БД и ИСС**

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н., доцент, А.С. Моляков

**6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)****Структура дисциплины (модуля) для очной формы обучения**

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 48 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 открытых ключей	6	2					10	Опрос
2	Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов	6	2					10	Опрос. Защита лабораторных работ.
3	Структура цифровых сертификатов	6	4			4		8	Опрос. Защита лабораторных работ.
4	Функции удостоверяющего центра	6	4			4		6	Опрос. Защита лабораторных работ.
5	Использование функций провайдера криптографических услуг	6	4			4		14	Опрос. Защита лабораторных работ.
	зачёт								Зачёт по билетам
	итого:		16			12		48	

**7. Обновление основной и дополнительной литературы (2020 г.)**

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

Дополнить раздел Основная литература

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

Дополнить раздел Основная литература

Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для вузов / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 320 с. — (Высшее образование). — ISBN 978-5-534-09964-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/455239>

Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450234>

Дополнить раздел Дополнительная литература

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>

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>

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>

8. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

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

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

9. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

#### Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global

	SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

**Состав программного обеспечения (ПО)**

№п /п	Наименование ПО	Производитель	Способ распространения ( <i>лицензионное или свободно распространяемое</i> )
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

К.т.н., доцент, А.С. Моляков