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

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ, УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ, УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ
Рабочая программа дисциплины

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 14.03.2024 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: изучение инфраструктуры открытых ключей, освоение принципов формирования электронной подписи, выработка умений настройки компонентов инфраструктуры.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	*ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик*	*Знать: оценки работоспособности применяемых средств защиты информации с использованием прикладного ПО Crypto Pro и ХСА*
	ПК-6.2 Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	*Уметь: оценить эффективности применяемых средств защиты информации с использованием прикладного ПО Crypto Pro и ХСА*
	ПК-6.3 Владеет навыками определения уровня защищенности и доверия средств защиты информации	*Владеть: навыками определения уровня защищенности и доверия средств защиты информации на примере ПО VeraCrypt и Crypto Pro*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Инфраструктура открытых ключей, удостоверяющие центры» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.
Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: "Математические основы защиты информации".
В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: "Безопасность программного обеспечения автоматизированных систем".

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	**28**
3	Практические занятия	**36**
	Всего:	**64**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 44 академических часа.

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 компонентом PKI: он является доверенной третьей стороной (trusted third party) это сервер, который осуществляет управление жизненным циклом сертификатов (но не их непосредственным использованием).
2	**Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов**	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. Репозиторий — хранилище, содержащее сертификаты и списки отозванных сертификатов (COC) и служащее для распространения этих объектов среди пользователей. В Федеральном Законе РФ № 63 «Об электронной подписи» он называется реестр сертификатов ключей подписей.

3	**Структура цифровых сертификатов**	Структура сертификата • Версия • Серийный номер • Идентификатор алгоритма подписи • Имя издателя • Период действия • Имя субъекта • Информация об открытом ключе субъекта: • Алгоритм открытого ключа • Открытый ключ субъекта • Уникальный идентификатор издателя (обязательно только для v2 и v3) • Уникальный идентификатор субъекта (обязательно только для v2 и v3) • Дополнения (для v2 и v3) • Возможные дополнительные детали • Алгоритм подписи сертификата (обязательно только для v3) • Подпись сертификата (обязательно для всех версий)
4	**Функции удостоверяющего центра**	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 информации, 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 PKI), один удостоверяющий центр может работать с несколькими регистрационными центрами. Иногда, удостоверяющий центр выполняет функции регистрационного центра.
5	**Использование функций провайдера криптографических услуг**	Архив сертификатов — хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком действия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы. Центр запросов — необязательный компонент системы, где конечные пользователи могут запросить или отозвать сертификат. Конечные пользователи — пользователи, приложения или системы, являющиеся

		владельцами сертификата и использующие инфраструктуру управления открытыми ключами.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	*Компоненты инфраструктуры открытых ключей*	*Лекция 1.* Самостоятельная работа	*Традиционная с использованием презентаций* *Изучение материалов лекций, тестирование*
2	*Нормативно-методическая база использования электронной подписи для придания юридической значимости электронных документов*	*Лекция 2.* Самостоятельная работа	*Традиционная с использованием презентаций* *Изучение материалов лекций, тестирование*
3	*Структура цифровых сертификатов*	*Лекция 3.1* *Лекция 3.2* *Практическое занятие 1.* Самостоятельная работа	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций, тестирование*
4	*Функции удостоверяющего центра*	*Лекция 4.1* *Лекция 4.2* *Практическое занятие 2.* Самостоятельная работа	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций, тестирование*
5	*Использование функций провайдера криптографических услуг*	*Лекция 5.1* *Лекция 5.2* *Практическое занятие 3.* Самостоятельная работа	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций, тестирование*

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

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

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

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– тестирование (темы 1-5)* *– практическое задание (темы 3)* *– практическое задание (темы 4-5)*	 *5 баллов* *6 баллов* *7 баллов*	 *30 баллов* *6 баллов* *14 баллов*
Промежуточная аттестация – *зачёт (зачет по билетам)*		*40 баллов*
Итого за дисциплину		*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	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ C	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Примерные контрольные вопросы для зачёта

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 PKI.
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 PKI.
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 PKI.
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

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/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ [Электронный ресурс] : Режим доступа : 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/, свободный. – Загл. с экрана.
5. Приказ ФСБ России от 27.12.2011 N 796 (ред. от 13.04.2022) "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра" [Электронный ресурс]. – Режим доступа : https://www.consultant.ru/document/cons_doc_LAW_126209/, свободный в комм. версии. – Загл. с экрана.

Литература

Основная

1. Игнатьев, Е. Б. Защита информации: криптоалгоритмы хеширования / Е. Б. Игнатьев. — Санкт-Петербург : Лань, 2023. — 264 с. — ISBN 978-5-507-45962-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/311792
2. Рацеев, С. М. Математические методы защиты информации и их основы. Сборник задач / С. М. Рацеев. — Санкт-Петербург : Лань, 2023. — 140 с. — ISBN 978-5-507-45197-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292913
3. Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 544 с. — ISBN 978-5-507-47085-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/326153
4. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401.
5. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563.
6. Волчков, В. П. Теория и методы криптографической защиты информации : учебное пособие / В. П. Волчков, В. Г. Санников. — Москва : МТУСИ, 2021 — Часть 1 — 2021. — 77 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/215195.

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.
   Центр разработки Криптоком [Электронный ресурс]: Режим доступа: http://www.cryptocom.ru/products/index.html/, свободный. – Загл. с экрана.
   Национальная электронная библиотека (НЭБ) www.rusneb.ru
   ELibrary.ru Научная электронная библиотека www.elibrary.ru
   Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

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

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

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

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Microsoft Share Point 2010
6. Vmware Player 15.5 +
7. Гостевая ОС CentOS 7
8. демо-дистрибутивы СКЗИ «Крипто-Про».

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

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

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.

Практическое занятие 1(12 ч.). Исследование механизмов защиты ЭП - проверка сформированности компетенций ПК-6

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.

Практическое занятие 2(12 ч.). Структура цифровых сертификатов. Ознакомления студентов с обязательными и дополнительными полями сертификатов - проверка сформированности компетенций ПК-6

Цель работы: получение практических навыков работы с сертификатами.
Указания по выполнению задания: обратить внимание на дополнительные поля сетификата.
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.

Практическое занятие 3(14 ч.). Использование функций провайдера криптографических услуг. Приобретение студентами навыков работы с утилитами СКЗИ «Крипто-Про» - проверка сформированности компетенций ПК-6

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.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Инфраструктура открытых ключей, удостоверяющие центры» реализуется на факультете информационных систем и безопасности 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 следующей компетенции:

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

В результате освоения дисциплины обучающийся должен:

- Знать оценки работоспособности применяемых средств защиты информации с использованием прикладного ПО Crypto Pro и XCA;
- Уметь оценить эффективности применяемых средств защиты информации с использованием прикладного ПО Crypto Pro и XCA;
- Владеть навыками определения уровня защищенности и доверия средств защиты информации на примере ПО VeraCrypt и Crypto Pro.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.
Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.