

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»  
Институт математики, физики и информационных технологий  
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:  
Директор института



Н. Л. Королева  
«05» июля 2021 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.В.ДВ.04.2 Современные технологии обеспечения информационной безопасности

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

**Автор программы:**

Анурьева Мария Сергеевна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	13
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	26
6. Учебно-методическое и информационное обеспечение дисциплины.....	28
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	29

## 1. Цели и задачи дисциплины

### 1.1 Цель дисциплины – формирование компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

### 1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

### 1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	На основе современных технологий обеспечений информационной безопасности администрирует средства защиты информации прикладного и системного программного обеспечения для обеспечения безопасности программ и данных

### 1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		2	6	7	8
1	Защита программ и данных			+	
2	Избранные вопросы информационной безопасности		+	+	
3	Преддипломная практика				+
4	Теоретические основы защиты информации	+			
5	Теоретические основы защиты информации на английском языке	+			

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Современные технологии обеспечения информационной безопасности» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Современные технологии обеспечения информационной безопасности» изучается в 2 семестре.

### 3.Объем и содержание дисциплины

#### 3.1.Объем дисциплины:

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>72</b>
Контактная работа	48
Лекции (Лекции)	16
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	24
Зачет	-

#### 3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
2 семестр					
1	Обеспечение информационной безопасности на основе отечественных разработок	2	4	3	Вопросы для самоподготовки / Лабораторная работа; Тестирование
2	Безопасность "Интернета вещей"	2	4	3	Тестирование; Вопросы для самоподготовки / Лабораторная работа
3	Безопасность "Больших данных"	2	4	3	Тестирование
4	Платежные системы и обеспечение их информационной безопасности	2	4	3	Вопросы для самоподготовки / Лабораторная работа; Тестирование
5	ГосСОПКА	2	4	4	Тестирование; Вопросы для самоподготовки / Лабораторная работа
6	Стандарты информационной безопасности	3	6	4	Тестирование

7	Анализ существующих и перспективных средств защиты информации	3	6	4	Вопросы для самоподготовки / Лабораторная работа; Тестирование
---	---------------------------------------------------------------	---	---	---	----------------------------------------------------------------------

## Тема 1. Обеспечение информационной безопасности на основе отечественных разработок (ПК-3)

### Лекция.

Правовое обеспечение информационной безопасности РФ должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов РФ при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере

### Лабораторные работы.

Лабораторная работа Astra linux Special Edition:

Работа с учётными записями пользователей и группами.

Цель работы:

Изучить особенности администрирования локальных учётных записей пользователей и групп в ОССН с использованием командной строки и графического интерфейса.

Порядок выполнения работы:

Порядок выполнения работы

1. Начать работу со входа в ОССН в графическом режиме с учётной записью пользователя user(уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).
2. Запустить терминал Fly из меню «Системные».
3. Определить текущую учётную запись пользователя с использованием команды `whoami`.
4. Проверить наличие права доступа на чтение к файлу `/etc/passwd` и получить следующие данные, выполнив команды `cat/etc/passwd` или `less/etc/passwd`: число параметров учётных записей пользователей (для этого дополнительно можно использовать команды `wc` и `sort`); текущее число учётных записей пользователей; число различных используемых командных интерпретаторов.
5. Вывести строку, соответствующую текущей учётной записи пользователя, из файла `/etc/passwd` с использованием команды `cat/etc/passwd|grep "^$(whoami):"`, при этом получить следующие данные: наличие пароля или свёртки пароля (вывести эти данные командой `cat/etc/passwd|grep "^$(whoami):" |cut -d:-f2`): `root@astra:/home/user# cat/etc/passwd|grep "^$(whoami):" root:x:0:0:root:/root:/bin/bash root@astra:/home/user# exit exit user@astra:~$ cat/etc/passwd|grep "^$(whoami):" user:x:1000:1000:,,,:/home/user:/bin/bash` группа и идентификатор текущей учётной записи пользователя; командный интерпретатор по умолчанию для текущей учётной записи пользователя.
6. найти отличия исполняемых файлов `adduser` и `useradd`, для чего: определить расположение файлов `adduser` и `useradd` с использованием команд `sudo which`, `adduser` и `sudo which useradd`; вывести в терминал Fly тип обоих файлов командой `file`, определить их принципиальное отличие.
7. Добавить две учётные записи пользователей `user1` и `user2` (с соответствующими домашними каталогами) с использованием команд `sudo adduser user1` и `sudo adduser user2`.

8. Проанализировать изменения в ОССН, связанные с добавлением новых учётных записей пользователей, для чего определить: домашние каталоги учётных записей пользователей по данным файла `/etc/passwd`; номер алгоритма свёртки паролей учётных записей пользователей по файлу `/etc/shadow` с использованием привилегированного режима или команды `sudo`:

`root@astra:/home/user#cat/etc/shadow|grep "^user:"|cut -d$ -f26` скрипты, которые были перемещены в домашние каталоги учётных записей пользователей из каталога `/etc/skel`, при этом сравнить файлы в каталоге `/etc/skel` с файлами домашних каталогов учётных записей пользователей с использованием команды `sudo diff -s /etc/skel/home/имя_пользователя|grep "идентичны"`; новые группы в файле `/etc/group`, идентификаторы новых учётных записей пользователей и групп в файлах `/etc/group` и `/etc/passwd`.

9. Осуществить попытку создания учётных записей пользователей `user3`, `user4` командами `useradd user3` и `useradd user4` без использования команды `sudo`, проанализировать результат. Выполнить те же действия с применением команды `sudo`, после чего определить: домашние каталоги учётных записей пользователей по файлу `/etc/passwd`; были ли созданы домашние каталоги учётных записей пользователей; наличие свёрток паролей учётных записей пользователей по файлам `/etc/passwd` и `/etc/shadow`, новые группы в файле `/etc/group` идентификаторы новых учётных записей пользователей в файле `/etc/passwd`; командный интерпретатор по умолчанию для созданных учётных записей пользователей: `root@astra:/home/user# tail -1 /etc/passwd|cut -d: -f7 /bin/bash`

10. Реализовать попытки задать пароль для учётных записей пользователей `user3` и `user4` с использованием команд `passwd user3` и `passwd user4` без использования и с использованием команды `sudo`, сравнить результаты. Определить алгоритм свёртки пароля этих учётных записей пользователей по файлу `/etc/shadow`.

11. Выполнить дополнительную настройку ОССН для обеспечения возможности входа с учётной записью пользователя `user3`, для чего осуществить следующие действия: выполнить вход в ОССН с учётной записью пользователя `user3`, введя его имя и пароль, проанализировать предупреждения, выдаваемые ОССН; войти в ОССН с учётной записью пользователя `user`; создать домашний каталог учётной записи пользователя `user3` командами `sudo mkdir /home/user3`, и назначить ему необходимые права доступа: `sudo chown user3:user3 /home/user3`, `sudo chmod 750 /home/user3`; проверить возможность входа в ОССН с учётной записью пользователя `user3`; войти в ОССН с учётной записью пользователя `user`.

12. Запустить терминал Fly в «привилегированном» режиме командой `sudo Fly-term`.

13. Модифицировать параметры учётных записей пользователей: установить домашний каталог учётной записи пользователя `user1` командой `usermod -d /home/userone user1`; установить домашний каталог учётной записи пользователя `user2` командой `usermod -d /home/usertwo user2`; проверить содержимое каталога `/home` командой `ls -la` и определить отличия в результатах выполнения команды `usermod` на предыдущих этапах.

14. Осуществить последовательные попытки входа в ОССН с учётными записями созданных пользователей `user1` и `user2`, при этом выполнить следующие действия: проанализировать причины появления предупреждений при входе в ОССН с учётной записью пользователя `user1`, сравнить отличия в командах, использованных при модификации параметров учётных записей пользователей `user1` и `user2`; вернуть домашний каталог учётной записи пользователя `user1` командой `usermod -d /home/user1 user1`, рассмотреть результат её выполнения, проверить запись о домашнем каталоге в файле `/etc/passwd`; повторно установить домашний каталог пользователя `user1` командой `usermod -t -d /home/userone user1`, проверить результат; проверить возможность входа в ОССН с учётной записью пользователя `user1`, выйти из ОССН.

15. Войти в ОССН с учётной записью пользователя `user` (Уровень\_0, «Высокий»). Запустить графическую утилиту редактирования учётных записей пользователей «Политика безопасности» через меню «Панель управления» главного пользовательского меню.

16. Открыть раздел настройки локальных пользователей, и для созданных учётных записей пользователей `user1`, `user2`, `user3`, `user4` произвольно задать их параметры: максимальный и минимальный уровни доступа; минимальные и максимальные наборы неиерархических категорий; максимальный уровень целостности.

17. Настроить параметры учётной записи пользователя user2: установить минимальное число дней между сменой пароля — 180 дней и до выдачи предупреждения о смене пароля — 5 дней; выбрать максимальный уровень — «Уровень\_3»; проверить возможность задать минимальный или максимальный набор неиерархических категорий.
18. Войти в ОССН с учётной записью пользователя user2, выбрав уровень доступа «Уровень\_1». Проверить возможность выбора набора неиерархических категорий и уровня целостности. Создать в каталоге «Документы» файл 1.txt. Выйти из ОССН.
19. Войти в ОССН с учётной записью пользователя user2, выбрав уровень доступа «Уровень\_2». Создать в каталоге «Документы» файл 2.txt.
20. Проверить возможность чтения объектов файловой системы ОССН, владельцем которых является учётная запись пользователя user2 (на текущем уровне доступа «Уровень\_2»): открыть каталог «Документы» уровня доступа «Уровень\_1» (Компьютер/Домашний/маш/11i0c00x0t0x0/Документы); открыть файл 1.txt, проверив возможность его чтения или записи; выйти из ОССН.
21. Проверить наличие и возможность чтения объектов файловой системы ОССН, владельцем которых является учётная запись пользователя user2 на текущем уровне доступа («Уровень\_1»): войти в ОССН с учётной записью пользователя user2, выбрав уровень доступа «Уровень\_1»; проверить возможность открытия каталога «Документы» для уровня доступа «Уровень\_2» (Компьютер/Домашний/маш/12i0c0x0t0x0/Документы); выйти из ОССН.
22. Войти в ОССН с учётной записью пользователя user. Запустить графическую утилиту «Политика безопасности». Сравнить списки вторичных групп для учётных записей пользователей user, user1, user2, user3, user4, при этом определив: учётные записи пользователей, являющиеся администраторами (входящими в группу astra-admin); учётные записи пользователей, входящие в группу users.
23. Создать новую учётную запись пользователя user10: установить минимальное число дней между сменой пароля — 180 дней и число дней выдачи предупреждения до смены пароля — 5 дней; выбрать максимальный уровень доступа — «Уровень\_3», минимальный уровень доступа — «Уровень\_0», уровень целостности — «Высокий»; добавить в список вторичных групп группы astra-admin и ldap1n; проверить возможность входа в ОССН с учётной записью пользователя user10 с уровнями доступа «Уровень\_2» или «Уровень\_3» (уровень целостности «Низкий»).
24. Войти в ОССН с учётной записью пользователя user10 (уровень доступа — «Уровень\_0», уровень целостности «Высокий»), Проверить возможность создания новой учётной записи пользователя user11 с использованием графической утилиты Fly-admin-smc без использования и с использованием команды sudo. Выйти из ОССН.
25. Войти в ОССН с учётной записью пользователя user1 с уровнем доступа — «Уровень\_0». Осуществить попытки запуска графической утилиты «Политика безопасности» через главное пользовательское меню и запуска её с использованием терминала Fly командой Fly-admin-smc. Проанализировать результаты и предупреждения ОССН.
26. Осуществить переключение между сеансами различных учётных записей пользователей без выхода из ОССН: через меню «Завершение работы» главного пользовательского меню перейти в подменю «Сессия» и далее «Отдельная» и войти в ОССН с учётной записью пользователя user (уровень целостности «Высокий»); в аналогично вернуться и далее закрыть сеанс от имени учётной записи пользователя user1.
27. С использованием графической утилиты «Политика безопасности» заблокировать пароль учётной записи пользователя user1. Проверить изменения файлов /etc/passwd и /etc/shadow, осуществив следующие действия: в терминале Fly выполнить команды sudo cat /etc/passwd и sudo cat /etc/shadow; проверить наличие блокировки учётной записи пользователя по файлу /etc/shadow (должен быть установлен знак «!» в начале свёртки пароля); проверить функционирование блокировки путём осуществления попытки входа в ОССН в отдельном сеансе от имени учётной записи пользователя user1; снять блокировку (выполнить удаление пароля и блокировки входа, задать повторно пароль) и проверить возможность входа в ОССН с учётной записью пользователя user1.



28. Выполнить удаление учётных записей пользователей: удалить учётную запись пользователя user10 с использованием графической утилиты «Политика безопасности»; удалить учётную запись пользователя user2 командой `sudo deluser user2`; удалить учётную запись пользователя user1 командой `sudo userdel user1`; проверить наличие домашних каталогов учётных записей пользователей user1 и user2, после чего с использованием справочной информации по команде `userdel` определить её параметры, позволяющие удалять содержимое домашнего каталога учётной записи пользователя; удалить домашние каталоги учётных записей пользователей user1 и user2 непосредственно командами `rm -r /home/userone` и `rm -r /home/usertwo`, осуществив попытки удаления без использования и с использованием команды `sudo`; проверить наличие домашних каталогов учётных записей пользователей user1, user2 и user10 в каталоге `/home/.pdp`.

29. Создать новую группу group3 (с использованием графической утилиты «Политика безопасности») и группу group4 (командой `sudo addgroup group4`, выполненной в терминале Fly).

30. Добавить учётную запись пользователя user3 во вторичную группу group3 командой `usermod -a -G group3 user3` и во вторичную группу group4 с помощью графической утилиты «Политика безопасности». Проверить включение учётной записи пользователя user3 в группы group3 и group4 путем просмотра содержимого файла `/etc/group` командами `cat/etc/group|grep "group3"` и `cat/etc/group|grep "group4"`.

31. Выполнить удаление учётной записи пользователя user3 из группы group3 с использованием графической утилиты «Политика безопасности» и из группы group4 командой `gpasswd -d user3 group4`.

32. Удалить группу group3 командой `sudo delgroup group3` в терминале Fly и группу group4 с помощью графической утилиты «Политика безопасности».

33. Изучить порядок хранения параметров мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей. Для этого выполнить следующие действия: определить уровни доступа, заданные в ОССН, для этого вывести в терминал Fly содержимое файла `/etc/passwd/mac_levels`; определить иерархические категории, заданные в ОССН, для этого вывести в терминал Fly содержимое файла `/etc/passwd/mac_categories`; определить идентификатор учётной записи пользователя user1 по файлу `/etc/passwd` командой `cat/etc/passwd|grep "^user1:"|cut -d : -f3`; считать параметры мандатного управления доступом и мандатного контроля целостности для учётной записи пользователя user1 командой `cat/etc/passwd/macdb/$(cat/etc/passwd|grep "^user1:"|cut -d : -f3)` и проверить их соответствие данным, отображаемым в графической утилите «Политика безопасности».

### **Задания для самостоятельной работы.**

1. Составить полный перечень использованных команд с кратким описанием их назначения.
2. Составить список команд, которые были использованы в ходе работы с описанием результатов их выполнения.
3. Описать порядок работы с графической утилитой «Политика безопасности» (Flyadmin-smc) при осуществлении следующих действий: создание новой учётной записи пользователя или группы; удаление существующих учётной записи пользователя или группы; добавление учётной записи пользователя в существующую группу; добавление учётной записи пользователя в группу администраторов (astra-admin); изменение параметров мандатного управления доступом и мандатного контроля целостности.
4. Составить список и назначение системных файлов, связанных с хранением параметров учётных записей пользователей, групп, параметров мандатного управления доступом и мандатного контроля целостности.

## **Тема 2. Безопасность "Интернета вещей" (ПК-3)**

### **Лекция.**

В наши дни «Интернет вещей» является весьма популярной темой: конференции, на которых затрагиваются вопросы безопасности и выступают компании, производящие оборудование или программное обеспечение, проходят чуть ли не еженедельно, новые решения постоянно освещаются в специализированных изданиях. Компания Avnet Silica также считает необходимым принять участие в обсуждении этой важной и интересной темы. В статье разъясняется, что именно, по мнению специалистов Avnet, скрывается за понятием «безопасность «Интернета вещей», а также перечислены реальные проблемы клиентов компании, которые касаются таких аспектов, как аппаратные средства и встроенное либо серверное программное обеспечение (ПО). Решения, обеспечивающие безопасность «Интернета вещей», представлены в том ключе, как Avnet представляет его развитие в течение ближайших 6–8 лет, т. е., пока наш мир не перейдет полностью на протоколы IPv6 и 6LoWPAN.

### **Лабораторные работы.**

Лабораторная работа вещи и их взаимодействия №1:

Дается понятие Интернет вещей, рассматриваются процессы в моделях управляемых систем, исследуются модели и методы коммуникаций и архитектура Интернет вещей.

Ход работы:

- 1 Сравнение систем контроля с открытым и закрытым контурами
- 2 Рисование диаграммы процессов
- 3 Схема реального процесса
- 4 Анализ процесса
- 5 Система контроля с открытым контуром
- 6 Соединение устройств для создания IoT

### **Задания для самостоятельной работы.**

1. Поясните основные способы взаимодействия с интернет-вещами
2. Основные характеристики подхода «большие данные»
3. В чем суть идеи повсеместной компьютеризации?
4. Основные направления практического внедрения IoT.
5. Базовые принципы IoT.

## **Тема 3. Безопасность "Больших данных" (ПК-3)**

### **Лекция.**

Big Data («большие данные») в информационной безопасности – механизм использования технологии больших данных, при котором для решения задач обеспечения безопасности накапливаются и анализируются данные, полученные из разнородных (структурированных и неструктурированных) источников и отличающиеся большим объемом и скоростью обновления. Данные могут поступать из информационных и бизнес-систем, систем управления и связи, с устройств и датчиков.

В качестве инструмента обеспечения информационной безопасности большие данные обладают огромным потенциалом, а их использование приобретает особую актуальность в связи с распространением облачных сервисов и взаимосвязанных устройств. Увеличение объемов поступающей информации при условии их своевременного и точного анализа позволяет получить более объективное представление о процессах информационной безопасности, повысить осведомленность о наличии либо отсутствии угроз и об их характере и, как следствие, предпринимать более эффективные меры по их ликвидации.

### **Лабораторные работы.**

1. Установка одноузлового кластера Hadoop в Linux Astra SE.

2. Программирование в Hadoop: программа MapReduce для подсчета слов с использованием Eclipse.
3. Реализация умножения матриц с использованием одного шага Map-Reduce.
4. Реализация реляционного алгоритма на Pig
5. Реализация операций с базой данных в Hive.

#### **Задания для самостоятельной работы.**

1. Каким образом реализуется фильтрация Блума с помощью MapReduce?
2. Реализация алгоритма набора часто задаваемых элементов с помощью MapReduce?
3. Изучите реализацию алгоритма кластеризации с использованием MapReduce.
4. Реализуйте алгоритм Page Rank с использованием MapReduce.

### **Тема 4. Платежные системы и обеспечение их информационной безопасности (ПК-3)**

#### **Лекция.**

Вопросы безопасности электронных платежных систем являются сложной задачей для финансового сектора и регуляторов. Существуют две серьезные проблемы – несанкционированные списания средств с банковских карт или счетов юридических лиц и общая гарантия сохранности платежей, совершаемых через небанковские системы переводы платежей. Принимаемые в последние годы меры смогли сделать электронные переводы более безопасными.

#### **Лабораторные работы.**

1. Ознакомиться с созданием анонимного кошелька и работой ГПЦ.
2. Ознакомиться с платежной системой " Мир ".
3. Ознакомиться с платежной системой " SWIFT ".

#### **Задания для самостоятельной работы.**

1. Процедура контроля, состоящая из идентификации и проверки выполнения каждого перевода с помощью трех показателей, определяющих платежные системы
2. Платежная карточка, которая дает возможность ее держателю проводить операции за счет средств, учитываемых на карточном счете юридического лица
3. Из каких основных элементов состоит НСМЭП?
4. Из каких основных элементов состоит ГПЦ (главный процессинговый центр)?
5. Для чего предназначены Электронные кошельки?

### **Тема 5. ГосСОПКА (ПК-3)**

#### **Лекция.**

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, создаваемая в целях предотвращения и устранения последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации. Она представляет собой иерархически взаимодействующие государственные и коммерческие центры, которые непрерывно делятся информацией о зафиксированных инцидентах и способах противодействия им.

#### **Лабораторные работы.**

1. Рассмотреть "ГосСОПКА".
2. Рассмотреть варианты подключения к ГосСОПКА.
3. Рассмотреть функции и задачи ГосСОПКА.

#### **Задания для самостоятельной работы.**

1. Какие существуют варианты подключения к ГосСОПКА?
2. Кто является участниками ГосСОПКА?
3. В чем различия между субъектом ГосСОПКА и субъектом КИИ?
4. Задачи ГосСОПКА?
5. Срок, в который субъект КИИ должен передать информацию в ГосСОПКА?

### **Тема 6. Стандарты информационной безопасности (ПК-3)**

### **Лекция.**

Проблемой информационной компьютерной безопасности начали заниматься с того момента, когда компьютер стал обрабатывать данные, ценность которых высока для пользователя. С развитием компьютерных сетей и ростом спроса на электронные услуги ситуация в сфере информационной безопасности серьезно обострилась, а вопрос стандартизации подходов к ее решению стал особенно актуальным как для разработчиков, так и для пользователей ИТ-средств.

Международные стандарты информационной безопасности

Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью - Информационные технологии» («Information technology -Information security management») является одним из наиболее известных стандартов в области защиты информации.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;

### **Лабораторные работы.**

1. Выбрать один стандарт информационной безопасности который используется в Российской Федерации и составить отчёт.
2. Выбрать один стандарт информационной безопасности который используется в зарубежных странах и составить отчёт.

### **Задания для самостоятельной работы.**

- 1 Основные руководящие документы.
- 2 Основные нормативные документы.
- 3 Перечислить международные стандарты.
- 4 Перечислить государственные (национальные) стандарты Российской Федерации.

## **Тема 7. Анализ существующих и перспективных средств защиты информации (ПК-3)**

### **Лекция.**

Проблема защиты информации от постороннего доступа и нежелательных воздействий на нее возникла давно, с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком. С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и в дальнейшем расширением масштабов человеческой деятельности информация приобретает цену. Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцу получить какой-либо выигрыш: материальный, политический, военный и т.д

### **Лабораторные работы.**

1. Выбрать одно средство защиты информации, составить отчёт (Преимущества этого средства, какие функции выполняет это средство, недостатки).

### **Задания для самостоятельной работы.**

1. Какие существуют недостатки и требования к современным средствам защиты?
2. Какие существуют методы защиты информации от аварийных ситуаций?

3. Какие существуют методы контроля доступа к внутреннему монтажу аппаратуры, линиям связи и технологическим органам управления?

#### 4. Контроль знаний обучающихся и типовые оценочные средства

##### 4.1. Распределение баллов:

2 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

##### Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
---------	------------------------------------	---------------------------------	--------------------	--------------------------------------

1.	Обеспечение информационной безопасности на основе отечественных разработок	Вопросы для самоподготовки / Лабораторная работа	6	<p>Методика оценки самоподготовки студентов.</p> <p>6 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>2 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>0,1 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul> <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> <li>1. Степень соответствия выполненного задания поставленным требованиям;</li> <li>2. Структурирование и комментирование лабораторной работы;</li> <li>3. Уникальность выполнения работы (отличие от работ коллег);</li> <li>4. Успешные ответы на контрольные вопросы.</li> </ol> <p>«4 балл» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«2 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p>
		Тестирование	8	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 8 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>
2.	Безопасность "Интернета вещей"	Тестирование	8	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 8 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>

		Вопросы для самоподготовки / Лабораторная работа	6	<p>Методика оценки самоподготовки студентов.</p> <p>6 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>2 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>0,1 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul> <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> <li>1. Степень соответствия выполненного задания поставленным требованиям;</li> <li>2. Структурирование и комментирование лабораторной работы;</li> <li>3. Уникальность выполнения работы (отличие от работ коллег);</li> <li>4. Успешные ответы на контрольные вопросы.</li> </ol> <p>«4 балл» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«2 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p>
3.	Безопасность "Больших данных"	Тестирование(контрольный срез)	10	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 10 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>

4.	Платежные системы и обеспечение их информационной безопасности	Вопросы для самоподготовки / Лабораторная работа	6	<p>Методика оценки самоподготовки студентов.</p> <p>6 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>2 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>0,1 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul> <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> <li>1. Степень соответствия выполненного задания поставленным требованиям;</li> <li>2. Структурирование и комментирование лабораторной работы;</li> <li>3. Уникальность выполнения работы (отличие от работ коллег);</li> <li>4. Успешные ответы на контрольные вопросы.</li> </ol> <p>«4 балл» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«2 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p>
		Тестирование	8	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 8 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>
		Тестирование	8	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 8 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>
5.	ГосСОПКА	Тестирование	8	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 8 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>



		Вопросы для самоподготовки / Лабораторная работа	6	<p>Методика оценки самоподготовки студентов.</p> <p>6 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>2 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>0,1 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul> <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> <li>1. Степень соответствия выполненного задания поставленным требованиям;</li> <li>2. Структурирование и комментирование лабораторной работы;</li> <li>3. Уникальность выполнения работы (отличие от работ коллег);</li> <li>4. Успешные ответы на контрольные вопросы.</li> </ol> <p>«4 балл» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«2 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p>
6.	Стандарты информационной безопасности	Тестирование(контрольный срез)	10	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 10 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>

7.	Анализ существующих и перспективных средств защиты информации	Вопросы для самоподготовки / Лабораторная работа	6	<p>Методика оценки самоподготовки студентов.</p> <p>6 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>2 балла ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>0,1 балл ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul> <p>Основными критериями оценки выполненной студентом и представленной для проверки работы являются:</p> <ol style="list-style-type: none"> <li>1. Степень соответствия выполненного задания поставленным требованиям;</li> <li>2. Структурирование и комментирование лабораторной работы;</li> <li>3. Уникальность выполнения работы (отличие от работ коллег);</li> <li>4. Успешные ответы на контрольные вопросы.</li> </ol> <p>«4 балл» - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.</p> <p>«2 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.</p> <p>«1 балл» - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.</p> <p>Балл не начисляется, если оформление не соответствует требованиям, критерии не выдержаны, защита менее 61 % контрольных вопросов.</p>
		Тестирование	8	<p>Тестирование подразумевает 10 вопросов. За прохождение тестирования выставляются следующие баллы:</p> <ul style="list-style-type: none"> <li>- 90 % - 8 баллов;</li> <li>- 65 % - 5 баллов;</li> <li>- 50 % - 2 балла;</li> <li>- менее 50 % - балл не начисляется.</li> </ul>
8.	Посещаемость		10	<p>10 баллов – студент посетил все 100% занятий</p> <p>7-9 баллов – студент посетил не менее 80% занятий</p> <p>4-6 баллов – студент посетил не менее 50% занятий</p> <p>1-3 балла – студент посетил не менее 25% занятий</p> <p>Если студент посетил менее 25% занятий, баллы не начисляются</p>

9.	Премияльные баллы	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
10.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
11.	Итого за семестр	100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

#### 4.2 Типовые оценочные средства текущего контроля

##### Вопросы для самоподготовки / Лабораторная работа

###### Тема 1. Обеспечение информационной безопасности на основе отечественных разработок

1. Какие имеются особенности создания учётных записей пользователей с использованием команд `adduser`, `useradd` и графической утилиты «Политика безопасности» (Fly-admin-smc), в том числе: какой группе должна принадлежать учётная запись пользователя, чтобы была возможность выполнения команды `adduser`? какими командами создаётся учётная запись пользователя, и какие дополнительные параметры при этом вводятся? какие ограничения накладываются на пароль учётной записи пользователя при его создании? в какие группы автоматически добавляется учётная запись пользователя?
2. Как выполнять привилегированные команды?
3. Создаются ли домашние каталоги учётных записей пользователей при добавлении их с использованием графической утилиты «Политика безопасности»?
4. Создаются ли домашние каталоги учётных записей пользователей при их добавлении с использованием команд `adduser` и `useradd`?
5. Какие минимальный и максимальный уровни доступа задаются по умолчанию для учётных записей пользователей, создаваемых командами `adduser` и `useradd`?
6. Какими способами можно добавить или удалить учётную запись пользователя из группы?

###### Тема 2. Безопасность "Интернета вещей"

- 1 Роль сетевых подключений в "Интернете Вещей".
- 2 Конечные устройства и их роль в архитектуре "Интернета Вещей".

- 3 Основные тренды в развитии "Интернета Вещей" в Российской Федерации и мире.
- 4 Примеры успешного внедрения IoT-систем и сервисов в Российской Федерации.

#### Тема 4. Платежные системы и обеспечение их информационной безопасности

- 1 Что такое платежная система "Мир".
- 2 Что такое платежная система "СПФС".
- 3 Что такое платежная система "SWIFT".
- 4 Особенности платежной системы "Мир"
- 5 Особенности платежной системы "СПФС"
- 6 Особенности платежной системы "SWIFT".

#### Тема 5. ГосСОПКА

- 1 Какие пять основных подсистем центра ГосСОПКА?
- 2 Какие функции выполняет ГосСОПКА?
- 3 История создание ГосСОПКА ?
- 4 Для чего создавалась ГосСОПКА?
- 5 Как происходит взаимодействие субъекта КИИ и ГосСОПКА?

#### Тема 7. Анализ существующих и перспективных средств защиты информации

- 1 Какие существуют криптографические средства защиты информации?
- 2 Какие существуют средства защиты данных от НСД?
- 3 Какие существуют методы защиты информации?
- 4 Какие существуют угрозы информационной безопасности?

### Тестирование

#### Тема 1. Обеспечение информационной безопасности на основе отечественных разработок

1. Каким образом организовано хранение сущностей файловой системы ОССН, созданных процессами, обладающими различными уровнями доступа?
2. Где и в каком формате хранятся параметры мандатного управления доступом и мандатного контроля целостности, заданные в ОССН?
3. Где и в каком формате хранятся параметры мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей?
4. Какой командой задаётся максимальный набор неиерархических категорий для текущей учётной записи пользователя?
5. Каким образом осуществляется переход от текущего сеанса к сеансу, функционирующему от имени другой учётной записи пользователя?
6. Позволяют ли команды useradd и adduser задавать параметры мандатного управления доступом и мандатного контроля целостности для создаваемых учётных записей пользователей?

#### Тема 2. Безопасность "Интернета вещей"

- 1 Определение понятия "Интернет Вещей".
- 2 Примеры и основные области применения "Интернета Вещей".
- 3 История появления и развития "Интернета Вещей".
- 4 Основные факторы, повлиявшие на развитие "Интернета Вещей".

#### Тема 3. Безопасность "Больших данных"

- 1 Средства и инструменты хранения данных.
- 2 Разнородность и семантика данных.

- 3 Основные характеристики Больших Данных.
- 4 Средства и инструменты статической обработки данных.
- 5 Средства и инструменты потоковой обработки данных.
- 6 Средства и инструменты хранения данных.
- 7 Каким образом реализуется фильтрация Блума с помощью MapReduce?
- 8 Реализуйте алгоритма Page Rank с использованием MapReduce.

#### Тема 4. Платежные системы и обеспечение их информационной безопасности

- 1 Перечислить платежные системы в Российской Федерации.
- 2 Перечислить платежных систем в мире.
- 3 Перечислить альтернативных платежных систем.
- 4 Что такое "Платежные системы".
- 5 Как обеспечивается безопасность платежных систем.

#### Тема 5. ГосСОПКА

- 1 Как работает средства обнаружения
- 2 Как работает средства предупреждения
- 3 Как работает средства ликвидации
- 4 Как работает средства расшифровки (ППКА)
- 5 Как работает средства обмена информацией
- 6 Какие используются средства криптографической защиты каналов связи

#### Тема 6. Стандарты информационной безопасности

- 1 Какие стандарты информационной безопасности имеют классификации?
- 2 Что такое стандарты информационной безопасности и для чего они нужны?
- 3 Какие основные области стандартизации информационной безопасности?
- 4 Какие существуют российские стандарты информационной безопасности?

#### Тема 7. Анализ существующих и перспективных средств защиты информации

- 1 Как обеспечить безопасный физический доступ?
- 2 Как обеспечить безопасный доступ к данным?
- 3 Как есть способы защиты данных?
- 4 Какие основные задачи криптографии?
- 5 Какие основные принципы работы криптосистем?

### 4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

#### Типовые вопросы зачета (ПК-3)

- 1 Понятие «информационные технологии». Определение.
- 2 Классификация информационных технологий.
- 3 Классификация программных средств.
- 4 Эволюция информационных технологий.
- 5 Свойства информационных технологий.
- 6 Виды информационных технологий. Их краткая характеристика.
- 7 Информационные технологии обработки данных.
- 8 Информационные технологии управления.
- 9 Информационные технологии автоматизации офиса.
- 10 Информационные технологии поддержки принятия решений.

- 11 Информационные технологии экспертных систем.
- 12 Перечислите современные информационные технологии коммуникации. Дайте их краткую характеристику.
- 13 Локальные сети Ethernet как физическая среда для построения информационных технологий.
- 14 Современная физическая среда для построения информационных технологий – оптоволоконные каналы.
- 15 Беспроводные коммуникации Bluetooth.
- 16 Технологии Wi-Fi.
- 17 Технологии WiMAX.
- 18 Мобильная связь на основе сотовых телефонных сетей.
- 19 Технологии использования спутникового интернета.
- 20 Телеконференции, электронная почта, IP-телефония, SIP операторы.

### Типовые задания для зачета (ПК-3)

1.

К негативным последствиям развития современных информационных и коммуникационных технологий можно отнести:

А)

формирование единого информационного пространства

Б)

работа с информацией становится главным содержанием профессиональной деятельности

В)

организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации

Г)

широкое использование информационных технологий во всех сферах человеческой деятельности

Д)

доступность личной информации для общества и государства, вторжение информационных технологий в частную жизнь людей

2.

Термин «информатизация общества» обозначает:

А)

целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий

Б)

увеличение избыточной информации, циркулирующей в обществе

В)

увеличение роли средств массовой информации

Г)

введение изучения информатики во все учебные заведения страны

Д)

организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации

3.

Развитый рынок информационных продуктов и услуг, изменение в структуре экономики, массовое использование информационных и коммуникационных технологий являются признаками:

А)

информационной культуры

Б)

высшей степени развития цивилизации

- В)  
информационного кризиса
- Г)  
информационного общества
- Д)  
информационной зависимости

4.

Методы обеспечения информационной безопасности делятся (указать неправильные ответ):

- А)  
правовые
- Б)  
организационно-технические
- В)  
политические
- Г)  
экономические
- Д)  
все перечисленные выше

5.

Обеспечение защиты информации проводится конструкторами и разработчиками программного обеспечения в следующих направлениях (указать неправильный ответ):

- А)  
защита от сбоев работы оборудования
- Б)  
защита от случайной потери информации
- В)  
защита от преднамеренного искажения
- Г)  
разработка правовой базы для борьбы с преступлениями в сфере информационных технологий
- Д)  
защита от несанкционированного доступа к информации

6.

Компьютерные вирусы – это:

- А)  
вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера
- Б)  
программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК
- В)  
программы, являющиеся следствием ошибок в операционной системе
- Г)  
пункты А) и В)
- Д)  
вирусы, сходные по природе с биологическими вирусами

7.

Отличительными особенностями компьютерного вируса являются:

- А)  
значительный объем программного кода
- Б)  
способность к самостоятельному запуску и многократному копированию кода

- В)  
 способность к созданию помех корректной работе компьютера
- Г)  
 легкость распознавания
- Д)  
 Пункты Б) и В)

8.

Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?

- А)  
 Уголовный кодекс РФ
- Б)  
 Гражданский кодекс РФ
- В)  
 Доктрина информационной безопасности РФ
- Г)  
 Постановления Правительства
- Д)  
 Указ Президента РФ

9.

Что не относится к объектам информационной безопасности Российской Федерации?

- А)  
 природные и энергетические ресурсы
- Б)  
 информационные ресурсы всех видов
- В)  
 информационные системы различного класса и назначения, информационные технологии
- Г)  
 система формирования общественного сознания
- Д)  
 права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности

10.

Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?

- А)  
 Неправомерный доступ к компьютерной информации
- Б)  
 Создание, использование и распространение вредоносных программ для ЭВМ
- В)  
 Умышленное нарушение правил эксплуатации ЭВМ и их сетей
- Г)  
 Все перечисленное выше
- Д)  
 Пункты Б) и В)

11.

Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?

- А)



Доктрина информационной безопасности РФ

Б)

Закон «О правовой охране программ для ЭВМ и баз данных»

В)

Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ

Г)

Указ Президента РФ

Д)

Закон «Об информации, информатизации и защите информации»

12.

Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?

А)

Закон «Об информации, информатизации и защите информации»

Б)

Закон «О правовой охране программ для ЭВМ и баз данных»

В)

Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ

Г)

Пункты А) и В)

Д)

Указ Президента РФ

13.

Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:

А)

Указ Президента РФ

Б)

Закон «Об информации, информатизации и защите информации»

В)

Закон «О правовой охране программ для ЭВМ и баз данных»

Г)

Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ

Д)

Доктрина национальной безопасности РФ

14.

Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?

А)

да, нарушено авторское право владельца сайта

Б)

нет, так как нормативно-правовые акты не являются объектом авторского права

В)

нет, если есть разрешение владельца сайта

Г)

да, нарушено авторское право автора документа

Д)

нет, если истек срок действия авторского права

15.

Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?

А)

можно, с указанием имени автора и источника заимствования

Б)

можно, с разрешения и автора статьи, и издателя

В)

можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения

Г)

можно, поскольку опубликованные статьи не охраняются авторским правом

Д)

можно, с разрешения издателя, издавшего данную статью, или автора статьи

#### 4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-3	Демонстрирует высокий уровень теоретических знаний методологического базиса решения задач защиты информации. Анализирует существующие методики определений требования к защите информации. Превосходно владеет знанием принципов обеспечения защиты информации. Способен продемонстрировать современные подходы к администрированию средств защиты информации прикладного и системного программного обеспечения.
«не зачтено» (0 - 49 баллов)	ПК-3	Не способен продемонстрировать знания методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Не владеет знанием принципов обеспечения защиты информации. Не способен продемонстрировать современные подходы к администрированию средств защиты информации прикладного и системного программного обеспечения.

### 5. Методические указания для обучающихся по освоению дисциплины (модуля)

#### 5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

## 5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

## 5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

## 5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы:
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Основная литература:

1. Тамб. гос. ун-т им. Г.Р. Державина Нормативное обеспечение информационной безопасности систем и организаций : инф. ресурс. - [Тамбов]: Изд-во ТГУ, 2008. - 1 электрон. опт. диск (CD-ROM).
2. Боброва, И. Л., Севрук, К. А. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем. - 2022-04-04; Методические указания и индивидуальные задания для самостоятельной работы по дисциплине . - Москва: Московский технический университет связи и информатики, 2015. - 35 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/61737.html>
3. Крутских А.В. Международная информационная безопасность. Теория и практика. В трех томах. Том 2. Сборник документов (на русском языке) : учебное пособие. - Москва: Аспект-Пресс, 2021. - 784 с. - Текст : электронный // ЭБС «Консультант студента вуза и медвуза [сайт]. - URL: <https://www.studentlibrary.ru/book/ISBN9785756710991.html>
4. Петренко В. И. Теоретические основы защиты информации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015. - 222 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

### 6.2 Дополнительная литература:

1. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза : монография. - М.: ЮНИТИ, Закон и право, 2012. - 159 с.
2. Чуянов, А. Г., Симаков, А. А. Обеспечение информационной безопасности в компьютерных системах : учебное пособие. - Весь срок охраны авторского права; Обеспечение информационной безопасности в компьютерных системах. - Омск: Омская академия МВД России, 2012. - 204 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/36015.html>

### 6.3 Иные источники:

1. Журнал «BIS Journal - Информационная безопасность банков» - <https://journal.ib-bank.ru/pub/169>
2. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
3. Федеральный портал "Российское образование" - <http://www.edu.ru/>
4. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>
5. Технические средства информационных технологий - <http://www.knigafund.ru>

6. Курс лекций по основам информатики - <http://www.intuit.ru/catalog/informatics/>

## **7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы**

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Kaspersky Endpoint Security 10 для Windows "Лаборатория Касперского" 26.07.2018

Microsoft Windows 10

Yandex браузер

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

2. Российская государственная библиотека. – URL: <https://www.rsl.ru>

3. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>

4. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>

5. Российская национальная библиотека. – URL: <http://nlr.ru>

6. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

### **Электронная информационно-образовательная среда**

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz)

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.