

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра №34

«УТВЕРЖДАЮ»

Руководитель направления

д.т.н., проф.

(должность, уч. степень, звание)



В.Ф. Шишлаков

(подпись)

«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Название дисциплины)

Код направления	27.03.04
Наименование направления/ специальности	Управление в технических системах
Наименование направленности	Управление и информатика в технических системах
Форма обучения	очная

Санкт-Петербург– 2021 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

проф., д.т.н., доц.

должность, уч. степень, звание

 24.06.21
подпись, дата

С.В. Беззатеев

инициалы, фамилия

Программа одобрена на заседании кафедры № 34

«24» июня 2021 г, протокол № 11

Заведующий кафедрой № 34

проф., д.т.н., доц.

должность, уч. степень, звание


 24.06.21
подпись, дата

С.В. Беззатеев

инициалы, фамилия

Ответственный за ОП 27.03.04(01)

должность, уч. степень, звание

 24.06.21
подпись, дата


Н.В. Решетникова

инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц., к.э.н., доц.

должность, уч. степень, звание

 24.06.21
подпись, дата

Г.С. Армашова-Тельник

инициалы, фамилия

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по направлению 27.03.04 «Управление в технических системах» направленность «Управление и информатика в технических системах». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общефессиональных компетенций:

ОПК-6 «способность осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий»,

ОПК-7 «способность учитывать современные тенденции развития электроники, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности»,

ОПК-9 «способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности».

Содержание дисциплины охватывает круг вопросов, раскрывающих сущность и значение информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме дифференцированного зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Дисциплина имеет своей целью: обеспечить выполнение требований, изложенных в федеральном государственном образовательном стандарте высшего профессионального образования. Изучение дисциплины направлено на формирование перечисленных ниже элементов профессиональных компетенций.

Также целями освоения дисциплины «Основы информационной безопасности» являются раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-6 «способность осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий»:

знать – методы поиска информации во внешних источниках

уметь – формализовать полученную информацию

владеть навыками – построения информационных моделей

иметь опыт деятельности – по решению задач по обработке информации

ОПК-7 «способность учитывать современные тенденции развития электроники, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности»:

знать – современные тенденции в области информационной безопасности

уметь - учитывать современные тенденции развития электроники, измерительной и вычислительной техники, информационных технологий в области информационной безопасности

владеть навыками – применения современных информационных технологий

иметь опыт деятельности – по работе с программными средствами

ОПК-9 «способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности»:

знать - методы информационных технологий

уметь - использовать навыки работы с компьютером

владеть навыками – оценки информационной безопасности объекта защиты

иметь опыт деятельности – в соблюдении основных требований информационной безопасности

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

Информатика
Информационные сети и телекоммуникации

Знания, полученные при изучении материала данной дисциплины, имеют самостоятельное значение

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	2/ 72	2/ 72
<i>Из них часов практической подготовки</i>		
<i>Аудиторные занятия, всего час., В том числе</i>	51	51
лекции (Л), (час)	34	34
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)		
<i>Самостоятельная работа, всего</i>	21	21
Вид промежуточного контроля: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Дифф. Зач.	Дифф. Зач.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Введение	4		2		4

Раздел 2. Сущность и понятие информационной безопасности	4		2		4
Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности	4		3		8
Раздел 4. Сущность и понятие защиты информации	4		2		8
Раздел 5. Состав и классификация носителей защищаемой информации	4		3		8
Раздел 6. Понятие и структура угроз защищаемой информации	4		2		8
Раздел 7. Объекты защиты информации	4		3		8
Раздел 8. Классификация видов, методов и средств защиты информации	6				17
Итого в семестре:	34		17		57
Итого	34	0	17	0	57

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	<p><i>Раздел 1. Введение.</i></p> <p>Предмет и задачи курса. Значение и место курса в подготовке специалистов, по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения курса.</p>
2	<p><i>Раздел 2. Сущность и понятие информационной безопасности</i></p> <p>Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия информационная безопасность".</p>
3	<p><i>Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности</i></p> <p>Значение информационной, безопасности для субъектов информационных отношений.</p> <p>Связь между информационной безопасностью и безопасностью информации.</p> <p>Понятие и современная концепция национальной безопасности. Место информационной, безопасности, в системе национальной безопасности.</p>

4	<p><i>Раздел 4. Сущность и понятие защиты информации</i></p> <p>Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части.</p> <p>Методологическая основа раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью.</p> <p>Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации".</p> <p>Способ реализации содержательной части защиты информации. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96. "Защита информации. Основные термины и определения".</p>
5	<p><i>Раздел 5. Состав и классификация носителей защищаемой информации</i></p> <p>Понятие носитель защищаемой информации". Соотношение между носителем и источником информации. Состав носителей защищаемой информации. Способы фиксации информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации. Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой информации.</p>
6	<p><i>Раздел 6. Понятие и структура угроз защищаемой информации</i></p> <p>Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.</p>
7	<p><i>Раздел 7. Объекты защиты информации</i></p> <p>Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.</p> <p>Состав объектов хранения письменных и видовых носителей информации, подлежащих защите. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения передачи информации. Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты.</p>
8	<p><i>Раздел 8. Классификация видов, методов и средств защиты информации</i></p> <p>Виды защиты информации, сферы их действия. Классификация методов защиты информации. Универсальные методы защиты информации, область их применения. Области применения организационных, криптографических и инженерно-технических методов защиты информации. Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.</p>

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего:					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7				
1.	Исследование генераторов паролей с заданными требованиями	2		2
2.	Построение модели угроз информационной системы	2		3
3.	Построение модели утечки информации информационной безопасности	2		4
4.	Исследование уязвимости информации	1		4
5.	Исследование видов уязвимости	1		5
6.	Исследование форм уязвимости	1		5
7.	Построение алгоритмов социальной инженерии и способы защиты от них	1		6
8.	Построение алгоритмов принятия решения	2		6
9.	Анализ обрабатываемой информации с точки зрения видов тайн и формирование требований к ее защите	2		7
10.	Анализ обрабатываемой информации с точки зрения ее защиты	1		8
11.	Сравнение криптографических и технических средств защиты.	2		8
Всего		17		

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	16	16
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)		
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	21	21

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 6-11.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.05В 75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	(74)
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с	(8)
Х Я 47	Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.	(9)
	http://e.lanbook.com/books/element.php?p11_id=3032	

	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с	
--	--	--

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 М 48	Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с.	(5)
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с.	(10)
	http://e.lanbook.com/books/element.php?pl1_id=4959 Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 с.	

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

URL адрес	Наименование
http://www.intuit.ru/studies/courses/10/10/info	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Дифференцированный зачёт	Список вопросов; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
	ОПК-6 «способность осуществлять поиск, хранение, обработку и анализ информации из

различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий»	
1	Информатика
6	Информационные сети и телекоммуникации
6	Производственная практика научно-исследовательская работа
6	Схемотехника средств контроля
7	Основы информационной безопасности
8	Производственная преддипломная практика
ОПК-7 «способность учитывать современные тенденции развития электроники, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности»	
5	Преобразовательные устройства систем управления
6	Микроконтроллеры
6	Производственная практика научно-исследовательская работа
7	Основы информационной безопасности
8	Производственная преддипломная практика
8	Расчет элементов систем управления
ОПК-9 «способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности»	
2	Информационные технологии
2	Учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности
5	Прикладное программирование
5	Системное программное обеспечение
6	Прикладное программирование
6	Производственная практика научно-исследовательская работа
7	Основы информационной безопасности
8	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4–балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	

$85 \leq K \leq 100$	«отлично» «зачтено»	<ul style="list-style-type: none"> - обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \leq K \leq 84$	«хорошо» «зачтено»	<ul style="list-style-type: none"> - обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \leq K \leq 69$	«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> - обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$K \leq 54$	«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> - обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Учебным планом не предусмотрено

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	<p>Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия.</p> <p>Сущность информационной безопасности. Объекты информационной безопасности</p> <p>Связь информационной безопасности с информатизацией общества</p> <p>Значение информационной, безопасности для субъектов информационных</p> <p>Место информационной, безопасности, в системе национальной безопасности.</p> <p>Существующие подходы к содержательной части понятия "защита информации"</p>

	<p>и способы реализации содержательной части</p> <p>Понятие уязвимости информации</p> <p>Методологическая основа раскрытия сущности и определения понятия защиты информации.</p> <p>Понятие носитель защищаемой информации". Соотношение между носителем и источником информации.</p> <p>Виды отображения информации в носителях</p> <p>Современные подходы к понятию угрозы защищаемой информации</p> <p>Понятие угрозы защищаемой информации.</p> <p>Понятие объекта защиты.</p> <p>Состав объектов хранения письменных и видовых носителей информации, подлежащих защите.</p> <p>Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты.</p> <p>Виды защиты информации, сферы их действия</p> <p>Классификация методов защиты информации</p> <p>Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.</p>

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)
Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	<p>1. СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:</p> <p>1. Информация</p> <p>2. Информационные технологии</p> <p>3. Информационная система</p> <p>4. Информационно-телекоммуникационная сеть</p> <p>5. Владелец информации</p> <p>2. ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:</p> <p>1. Информация</p> <p>2. Информационные технологии</p> <p>3. Информационная система</p> <p>4. Информационно-телекоммуникационная сеть</p> <p>5. Владелец информации</p> <p>3. ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:</p>

<ol style="list-style-type: none"> 1. Источник информации 2. Потребитель информации 3. Уничтожитель информации 4. Носитель информации 5. Обладатель информации <p>5. ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:</p> <ol style="list-style-type: none"> 1. База данных 2. Информационная технология 3. Информационная система 4. Информационно-телекоммуникационная сеть 5. Медицинская информационная система <p>6. ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:</p> <ol style="list-style-type: none"> 1. Электронное сообщение 2. Распространение информации 3. Предоставление информации 4. Конфиденциальность информации 5. Доступ к информации <p>7. ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:</p> <ol style="list-style-type: none"> 1. Уничтожение информации 2. Распространение информации 3. Предоставление информации 4. Конфиденциальность информации 5. Доступ к информации <p>8. ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:</p> <ol style="list-style-type: none"> 1. Сохранение информации 2. Распространение информации 3. Предоставление информации 4. Конфиденциальность информации 5. Доступ к информации <p>9. ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:</p> <ol style="list-style-type: none"> 1. Электронное сообщение 2. Информационное сообщение 3. Текстовое сообщение 4. Визуальное сообщение 5. SMS-сообщение <p>10. ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:</p> <ol style="list-style-type: none"> 1. Информационная система персональных данных 2. База данных 3. Централизованное хранилище данных 4. Система Статэкспресс 5. Сервер
--

11. К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:

1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. **Персональные данные**
5. Личная тайна

12. ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ...

1. «Об информации, информационных технологиях»
2. «О защите информации»
3. **Федеральным законом «О персональных данных»**
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера»

13. ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:

1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. **«Обработка персональных данных»**
5. «Изменение персональных данных»

14. ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:

1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. **Деперсонализация**

15. ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:

1. **Многопользовательские**
2. Однопользовательские
3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений

16. ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:

1. Авторизация
2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. **Идентификация**

17. ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:

1. Авторизация

2. Обезличивание
3. Деперсонализация
4. **Аутентификация**
5. Идентификация

18. ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ

1. **Авторизация**
2. Идентификация
3. Аутентификация
4. Обезличивание
5. Деперсонализация

19. ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:

1. Токен
2. Password
3. Пароль
4. **Login**
5. Смарт-карта

20. ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. **Шифрование**

21. ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

1. WWW
2. DICOM
3. **VPN**
4. FTP
5. XML

22. КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАНЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

1. Антивирус
2. Замок
3. **Брандмауэр**
4. Криптография
5. Экспертная система

23. ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:

1. Дисциплинарные взыскания
2. Административный штраф
3. Уголовная ответственность

4. Лишение свободы
5. **Смертная казнь**

24. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя

25. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

1. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица
4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

26. В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

1. Выход в Интернет без разрешения администратора
2. При установке компьютерных игр
3. В случаях установки нелегального ПО
4. В случае не выхода из информационной системы
5. **В любом случае неправомерного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности**

27. МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:

1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. **Да**
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомерных действий сотрудника

28. ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:

1. Идентификация
2. **Аутентификация**
3. Стратификация
4. Регистрация
5. Авторизация

29. НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:

1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. **Рядовые сотрудники предприятия**
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры

30. ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:

1. **Нет, не при каких обстоятельствах**
2. Нет, но для отправки срочных и особо важных писем можно
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

31. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ:

1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. **Конфиденциальная информация**
5. Документированная информация

32. ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:

1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. **Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)**
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК

33. ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН

1. **Содержать цифры и буквы, знаки препинания и быть сложным для угадывания**
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

34. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ...

1. Блокирование информации
2. Искажение информации
3. **Сохранность информации**
4. Утрату информации
5. Подделку информации

35. ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:

1. 1982
2. 1985
3. 1988
4. **1993**
5. 2005

36. ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ

1. **Конфиденциальная**
2. Персональная
3. Документированная

4. Информация составляющая государственную тайну
5. Информация составляющая коммерческую тайну

37. ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:

1. 1 главе Уголовного кодекса
2. 5 главе Уголовного кодекса
3. **28 главе Уголовного кодекса**
4. 100 главе Уголовного кодекса
5. 1000 главе Уголовного кодекса

38. В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ...

1. **О неправомерном доступе к компьютерной информации**
2. О создании, исполнении и распространении вредоносных программ для ЭВМ
3. О нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети
4. О преступлениях в сфере компьютерной информации
5. Об ответственности за преступления в сфере компьютерной информации

39. НА РИСУНКЕ ИЗОБРАЖЕНО...

1. **Настольная видеокамера**
2. Оптическая мышь
3. Телефонная трубка
4. Электронный замок
5. Аппаратный модули доверенной загрузки «Аккорд - АМДЗ»

40. ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:

1. **Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ**
2. Регулирование взаимоотношений в гражданском обществе РФ
3. Регулирование требований к работникам служб, работающих с информацией
4. Формирование необходимых норм и правил работы с информацией
5. Формирование необходимых норм и правил, связанных с защитой детей от информации

41. ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО...

1. **Несанкционированное копирование информации**
2. Утрата информации
3. Блокирование информации
4. Искажение информации
5. Продажа информации

42. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ...

1. Государство
2. Коммерческая организация
3. **Муниципальное учреждение**
4. Любой гражданин
5. Группа лиц, имеющих общее дело

43. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ...

1. **Простые люди**
2. Государство
3. Коммерческая организация
4. Муниципальное учреждение
5. Некоммерческая организация

44. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ...

1. Люди

2. **Государство**
3. Муниципальное учреждение
4. Учреждение
5. Некоммерческая организация

45. ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВЛАДЕЮТ:

1. **Государство**
2. Только образовательные учреждения
3. Только президиум Верховного Совета РФ
4. Граждане Российской Федерации
5. Только министерство здравоохранения

46. ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:

1. Государство
2. **Различные учреждения**
3. Государственная Дума
4. Граждане Российской Федерации
5. Медико-социальные организации

47. ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:

1. Государство
2. Различные учреждения
3. Государственная Дума
4. **Жители Российской Федерации**
5. Медико-социальные организации

48. ДОСТУП К ИНФОРМАЦИИ – ЭТО:

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
3. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
4. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
5. **Возможность получения информации и ее использования**

49. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:

1. **Конфиденциальная информация**
2. Документы офера и договоров
3. Факс
4. Личный дневник
5. Законы РФ

50. ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:

- a. Токен
- б. Password
- в. Пароль
- г. Login
- д. **Смарт-карта**

51. УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:

1. Токен
2. **Автономный токен**
3. USB-токен
4. Устройство iButton
5. Смарт-карта

52. ДОСТУП ПОЛЬЗОВАТЕЛЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ КОМПЬЮТЕРА И / ИЛИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ДОЛЖЕН РАЗРЕШАТЬСЯ ТОЛЬКО ПОСЛЕ:

1. Включения компьютера
2. **Идентификации по логину и паролю**
3. Запроса паспортных данных
4. Запроса доменного имени
5. Запроса ФИО

53. АППАРАТНЫЕ МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД - АМДЗ» ПРЕДСТАВЛЯЮТ СОБОЙ...

1. **Аппаратный контролер**
2. Электронный замок
3. Система контроля
4. Сетевой адаптер
5. Копировальный аппарат

54. ЭЛЕКТРОННЫЕ ЗАМКИ «СОБОЛЬ» ПРЕДНАЗНАЧЕНЫ ДЛЯ ...

1. **Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах**
2. Сканирования отпечатков пальцев
3. Проверки скорости и загрузки файлов
4. Общего контроля
5. Идентификации пользователя

55. Для защиты от злоумышленников необходимо использовать:

1. Системное программное обеспечение
2. Прикладное программное обеспечение
3. **Антивирусные программы**
4. Компьютерные игры
5. Музыка, видеофильмы

56. ФЕДЕРАЛЬНЫЙ ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ" ДАЕТ ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ:

1. Текст книги или письма
2. **Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**
3. Сведения о явлениях и процессах
4. Факты и идеи в формализованном виде
5. Шифрованный текст, текст на неизвестном языке

57. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ...

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. **Сохранности информации**
5. Преобразования информации

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий										
	<p>Задача 1. Парольная комбинация</p> <p>Для входа в систему используется пароль, состоящий из трёх двузначных чисел, расположенных следующим образом:</p> <p style="text-align: center;">xx-xx-xx</p> <p>Известно, что пароль состоит из 3-х неповторяющихся простых чисел. При этом, последняя цифра первого числа равна первой цифре второго числа, а последняя цифра второго числа равна первой цифре третьего числа.</p> <p>Пример:</p> <p style="text-align: center;">x1-17-7y</p> <p>Задержка между попытками входа в систему равна 1 секунде. За какое минимальное время (в секундах) можно гарантированно получить пароль, если на ввод пароля время не тратится, и количество попыток ввода пароля не ограничено?</p> <p>Задача 2. Сетевой трафик</p> <p>Был получен фрагмент сетевого трафика пользователя при взаимодействии с игровым сервером. Известно, что сервер работает по протоколу UDP и его порт назначения равен 8229. Структура UDP-дейтаграммы представлена ниже:</p> <table border="1" data-bbox="408 1328 1241 1424"> <thead> <tr> <th>2 байта</th> <th>2 байта</th> <th>2 байта</th> <th>2 байта</th> <th>...</th> </tr> </thead> <tbody> <tr> <td>UDP-порт отправителя</td> <td>UDP-порт получателя</td> <td>Длина UDP-дейтаграммы</td> <td>Контрольная сумма</td> <td>Данные</td> </tr> </tbody> </table> <p>Длина UDP-дейтаграммы включает в себя размер заголовка и размер данных в байтах.</p> <p>Дамп трафика:</p> <pre> 0B D7 20 25 00 16 1D DC 47 45 54 20 43 4F 4D 4D 41 4E 44 3A 20 25 20 25 0B D7 00 12 69 AF 53 45 54 20 43 4F 4F 52 44 3A 20 25 0B D7 00 12 25 C0 20 25 28 33 34 2C 35 34 29 00 0B D7 20 25 00 14 2C 8F 43 4F 4D 4D 41 4E 44 20 2D 20 4F 4B </pre> <p>Определите, какие данные сервер отправил клиенту.</p>	2 байта	2 байта	2 байта	2 байта	...	UDP-порт отправителя	UDP-порт получателя	Длина UDP-дейтаграммы	Контрольная сумма	Данные
2 байта	2 байта	2 байта	2 байта	...							
UDP-порт отправителя	UDP-порт получателя	Длина UDP-дейтаграммы	Контрольная сумма	Данные							

	<p>Задача 3. Шифрование</p> <p>В системе используется следующий алгоритм шифрования текстовых сообщений: значение каждого следующего байта циклически сдвигается побитно влево N раз, где N – значение предыдущего зашифрованного байта. Первый байт сообщения не шифруется.</p> <p>Расшифруйте предоставленный зашифрованный фрагмент текста:</p> <p>53 2B 73 23 01 C2 D5 8E 1A 80 72 95 2E 5D AC 37 3A</p>
--	---

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

1.1. Методические указания для обучающихся по освоению лекционного материала

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области дискретной математики. Создание поддерживающей образовательной среды преподавания служит участие студентов в конференциях, видеоконференциях, участие в научно-исследовательской работах обучающей кафедры.

Данная дисциплина предоставляет возможность студентам развивать и продемонстрировать навыки, используя методы комбинаторики, теории графов и теории автоматов, алгоритмическими процедурами решения задач оптимизации на дискретных структурах.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходиться к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);

Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Методические указания для обучающихся по прохождению лабораторных работ (если предусмотрено учебным планом по данной дисциплине)

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Обязательно для заполнения преподавателем

Структура и форма отчета о лабораторной работе

Обязательно для заполнения преподавателем

Требования к оформлению отчета о лабораторной работе

Обязательно для заполнения преподавателем

Если методические указания по прохождению лабораторных работ имеются в изданном виде, в виде электронных ресурсов библиотеки ГУАП, системы LMS, кафедры и т.д., необходимо дать на них ссылку или привести URL адрес.

Методические указания для обучающихся по прохождению курсового проектирования/ работы (если предусмотрено учебным планом по данной дисциплине)

Курсовой проект/ работа проводится с целью формирования у обучающихся опыта комплексного решения конкретных задач профессиональной деятельности.

Курсовой проект/ работа позволяет обучающемуся:

- систематизировать и закрепить полученные теоретические знания и практические умения по профессиональным учебным дисциплинам и модулям в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;
- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;
- углубить теоретические знания в соответствии с заданной темой;
- сформировать умения применять теоретические знания при решении нестандартных задач;
- приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;

- сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;
- сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;
- развить профессиональную письменную и устную речь обучающегося;
- развить системное мышление, творческую инициативу, самостоятельность, организованность и ответственность за принимаемые решения;
- сформировать навыки планомерной регулярной работы над решением поставленных задач.

Структура пояснительной записки курсовой работы / проекта

Обязательно для заполнения преподавателем

Требования к оформлению пояснительной записки курсовой работы / проекта

Обязательно для заполнения преподавателем

Если методические указания по прохождению курсовой работы / проекта имеются в изданном виде, в виде электронных ресурсов библиотеки ГУАП, системы LMS, кафедры и т.д., необходимо дать на них ссылку или привести URL адрес.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Если методические указания по прохождению самостоятельной работы имеются в изданном виде, в виде электронных ресурсов библиотеки ГУАП, системы LMS, кафедры и т.д., необходимо дать на них ссылку или привести URL адрес.

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой