

Подписано электронной подписью:

Вержицкий Данил Григорьевич

Должность: Директор КГПИ ФГБОУ ВО «КемГУ»

Дата и время: 2024-02-21 00:00:00

471086fad29a3b30e244e728abc3661ab35c9d50210def0e75e03a5b6fdf6436

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Кемеровский государственный университет»

Новокузнецкий институт (филиал)

федерального государственного бюджетного образовательного учреждения

высшего образования

«Кемеровский государственный университет»

Факультет информационных технологий

Кафедра информационных систем и управления

им. В.К. Буторина

УТВЕРЖДАЮ

Декан

 В.О. Каледин

« 13 » февраля 2017 г.

## Рабочая программа дисциплины

### **Б1.Б.19 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Направление подготовки

09.03.03 Прикладная информатика

Направленность (профиль) подготовки

Прикладная информатика в технике и технологиях

Уровень бакалавриата

Программа

Академический бакалавриат

Квалификация выпускника

Бакалавр

Форма обучения

очная

Год набора 2015

Новокузнецк 2017

## Содержание

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП БАКАЛАВРИАТА .....	4
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся .....	4
3.1. Объём дисциплины по видам учебных занятий (в часах) .....	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	5
4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах).....	5
4.2 Содержание дисциплины (модуля), структурированное по разделам (темам) .....	6
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю).....	11
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю) .....	11
6.1 Паспорт фонда оценочных средств по дисциплине (модулю).....	11
6.2. Типовые контрольные задания или иные материалы .....	12
6.2.1. Экзамен .....	12
6.2.2 Тест .....	13
6.2.3 Контрольная работа .....	17
6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	18
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля) .....	19
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины (модуля) .....	20
9. Методические указания для обучающихся по освоению дисциплины (модуля) .....	20
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости).....	20
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).....	21
12. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине .....	21

# 1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В условиях модернизации системы образования одной из основных задач высшей школы является формирование ключевых компетенций будущих выпускников. Компетентностный подход предполагает формирование интеллектуальной и исследовательской культуры студентов, создание условий для самоопределения и самореализации их потенциальных возможностей в процессе обучения.

Курс «Информационная безопасность» позволяет студентам ознакомиться с методами и средствами защиты информации в персональном компьютере и компьютерных сетях, изучить способы хранения и шифрования данных, проблемы несанкционированного межсетевых доступа к информации, современные средства криптографической защиты информации, вооружиться методами познания и сформировать познавательную самостоятельность.

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

<i>Коды компетенции</i>	<b>Результаты освоения ООП</b>	<b>Перечень планируемых результатов обучения по дисциплине</b>
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p><b>Знать:</b> роль и значение информации в развитии современного информационного общества; основные угрозы информационной безопасности; понятие государственной тайны; основные способы обеспечения информационной безопасности.</p> <p><b>Уметь:</b> соблюдать требования информационной безопасности.</p> <p><b>Владеть:</b> навыками и методами защиты конфиденциальных данных; различными видами алгоритмов криптографии данных; навыками администрирования и безопасной работы в компьютерных сетях.</p>
ПК-18	способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	<p><b>Знать:</b> виды угроз ИС и методы обеспечения информационной безопасности; модели безопасности и их применение.</p> <p><b>Уметь:</b> выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.</p> <p><b>Владеть:</b> основными положениями теории информационной безопасности информационных систем, навыками разработки политики безопасности.</p>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП БАКАЛАВРИАТА

Дисциплина Б1.Б.19 «Информационная безопасность» относится к базовой части ООП и участвует в формировании компетенций ОПК-4 и ПК-18 совместно с дисциплинами:

- Вычислительные системы, сети и телекоммуникации
- Сетевые технологии в экономике
- Итоговая государственная аттестация
- Практикум на ЭВМ
- Введение в специальность
- Информационные технологии в специальном образовании
- Современные информационные технологии

Дисциплина изучается на 4 курсе в 7 семестре очной формы обучения

## 3. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 5 зачетных единиц (ЗЕ), 180 академических часов.

### 3.1. ОБЪЁМ ДИСЦИПЛИНЫ ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ (В ЧАСАХ)

Объём дисциплины	Всего часов
	Очная форма
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54
Аудиторная работа (всего):	54
в т. числе:	
Лекции	18
Семинары, практические занятия	
Практикумы	
Лабораторные работы	36
Внеаудиторная работа (всего):	90
в том числе, индивидуальная работа обучающихся с преподавателем:	
Курсовое проектирование	
Групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем	
Творческая работа (эссе)	

Самостоятельная работа обучающихся (всего)	90
Вид промежуточной аттестации обучающегося ( <i>экзамен</i> )	<b>36,</b> экзамен

#### 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

##### 4.1. РАЗДЕЛЫ ДИСЦИПЛИНЫ (МОДУЛЯ) И ТРУДОЕМКОСТЬ ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ (В АКАДЕМИЧЕСКИХ ЧАСАХ)

##### *Очная форма обучения*

№ п/п	Раздел дисциплины	Общая трудоём- кость (часов)  всего	Виды учебных занятий, включая самостоятельную работу обуча- ющихся и трудоемкость (в часах)			Формы теку- щего контроля успеваемости
			аудиторные учебные занятия		самостоя- тельная ра- бота обуча- ющихся	
			лек- ции	Лаборатор- ные /практическ ие занятия		
1.	Введение в предмет. Угрозы информацион- ной безопасности	23	2	6	15	Устный доклад, тест
2.	Основные понятия тео- рии информационной безопасности	23	2	6	15	Устный доклад, тест
3.	Программно- технические методы защиты	25	4	6	15	Устный доклад, отчет по прак- тической рабо- те, тест
4.	Криптографические методы защиты	25	4	6	15	Устный доклад, отчет по прак- тической рабо- те, тест
5.	Организационно пра- вовые методы инфор- мационной безопасно- сти	25	4	6	15	Устный доклад, тест
6.	Роль стандартов в обеспечении информа- ционной безопасности	23	2	6	15	Устный доклад, тест
	Форма контроля	36				<b>Экзамен</b>
<b>ИТОГО</b>		<b>180</b>	<b>18</b>	<b>36</b>	<b>90</b>	

## 4.2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО РАЗДЕЛАМ (ТЕМАМ)

### Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание
1	Введение в предмет. Угрозы информационной безопасности	<p>Понятие информационной безопасности и защищенной системы. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.</p> <p>Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).</p> <p>Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.</p>
2	Основные понятия теории информационной безопасности	<p>Основные положения теории информационной безопасности информационных систем. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности.</p> <p>Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности.</p> <p>Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.</p>
3	Программно-технические методы защиты	<p>Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопас-</p>

№ п/п	Наименование раздела дисциплины	Содержание
		<p>ность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.</p> <p>Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.</p> <p>Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.</p> <p>Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.</p> <p>Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.</p>
4	Криптографические методы защиты	<p>Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.</p> <p>Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами).</p> <p>Использование криптографических средств для решения задач идентификация и аутентификация.</p> <p>Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.</p> <p>Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.</p>
5	Организационно правовые методы информационной безопасности	<p>Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопас-</p>

№ п/п	Наименование раздела дисциплины	Содержание
		ности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
6	Роль стандартов в обеспечении информационной безопасности	<p>Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.</p> <p>Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.</p> <p>Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.</p> <p>Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.</p>

## Содержание лабораторных работ

№	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в предмет. Угрозы информационной безопасности	Построение матрицы рисков для выбранного предприятия.
2	Основные понятия теории информационной безопасности	Знакомство с основными направлениями работ в рамках федеральной программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки ЭЦП.
3	Программно-технические методы защиты	Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.
4	Криптографические методы защиты	Методы современной криптографии на примере применения одного из предложенных алгоритмов.
5	Организационно правовые методы информационной безопасности	Проведение анализа способов нарушений безопасности на примере конкретного предприятия.
6	Роль стандартов в обеспечении информационной безопасности	Изучение логики работы и формы предоставления информации сетевыми анализаторами; овладение приемами анализа сетевого трафика; получение базовых знаний для обнаружения и организации сетевых атак.

## Содержание практических работ

№	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в предмет. Угрозы информационной безопасности	<p>Вопросы по теме:</p> <ol style="list-style-type: none"> <li>1. Какие принципы обеспечения целостности информации в ПК Вам известны?</li> <li>2. В чем заключаются особенности защиты в персональных компьютерах?</li> <li>3. Защита ПК от несанкционированного доступа</li> <li>4. Каким требованиям должен отвечать надежный пароль?</li> </ol>
2	Основные понятия теории информационной безопасности	<p>Вопросы по теме:</p> <ol style="list-style-type: none"> <li>1. Чем человек обменивается с другим человеком через машину или с машиной в автоматизированной системе?</li> <li>2. Всякая ли информация подлежит защите? Что является критерием при принятии решения о защите информации предприятия?</li> <li>3. В каком виде может быть представлена информация? Что включает в себя понятие «Машинное представление информации»?</li> <li>4. Какой алфавит нашел применение в электронных</li> </ol>

		<p>вычислительных машинах?</p> <p>5. Как может быть защищена информация без аппаратных и программных средств защиты?</p> <p>6. Что представляет собой локальная вычислительная сеть?</p>
3	Программно-технические методы защиты	<p>1. Какие угрозы информационной безопасности компьютерной системы могут оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней?</p> <p>2. Какие типы компьютерных вирусов Вам известны?</p> <p>3. Укажите основные признаки заражения ПК.</p> <p>4. Антивирусные программы и программы-ревизоры.</p> <p>5. Что такое компьютерный вирус и какими свойствами он обладает?</p> <p>6. Меры антивирусной профилактики.</p>
4	Криптографические методы защиты	<p>1. Что такое криптология?</p> <p>2. Что такое криптография?</p> <p>3. Что такое криптоанализ?</p> <p>4. Что такое ключ?</p> <p>5. Что собой представляет криптосистема?</p> <p>6. Дайте определение стойкости криптосистемы.</p> <p>7. Какие основные типы криптосистем Вы знаете?</p> <p>8. Объясните суть преобразований: перестановка и замена.</p> <p>9. Приведите пример табличной перестановки с использованием ключевого слова.</p> <p>10. Что собою представляет система шифрования с использованием таблицы Вижинера?</p> <p>11. Что собой представляет блочная симметричная криптографическая система?</p>
5	Организационно правовые методы информационной безопасности	<p>1. На чем основано правовое регулирование обеспечения безопасности предпринимательской деятельности?</p> <p>4. Допускается ли в Российской Федерации недобросовестная конкуренция?</p> <p>5. Какие документы предприятия не могут составлять коммерческую тайну?</p>
6	Роль стандартов в обеспечении информационной безопасности	<p>1. Приведите некоторые положения законодательных актов Российской Федерации, касающихся обеспечения безопасности предпринимательской деятельности.</p> <p>2. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Есть ли этому исключение?</p>

## **5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

*Цели самостоятельной работы:*

1. Систематизация, закрепление и расширение теоретических знаний студентов по избранной специальности.
2. Развитие навыков ведения самостоятельной работы и овладения методикой исследования.
3. Определение уровня теоретических знаний студентов, а также умение применять их для решения конкретных задач информационной безопасности.

Для обеспечения самостоятельной работы обучающихся по дисциплине разработано учебно-методическое обеспечение в составе:

1. Типовые задания для подготовки к соответствующим контрольным мероприятиям, приведенные в разделе 6 рабочей программы дисциплины (РПД) и учебно-методическом комплексе (УМК) по дисциплине.
2. Учебно-методический комплекс, находящийся в свободном доступе во внутренней сети вуза по адресу: \\led\litera\ ФИТ\ Кафедра информационных систем и управления \УМК

Состав УМК: РПД, методические указания по изучению дисциплины для студентов, папки с файлами «Курс лекций», «Задачи СРС», тестовые задания.

## **6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

### **6.1 ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции	Наименование оценочного средства
1.	Введение в предмет. Угрозы информационной безопасности	ОПК-4, ПК-18	Тест
2.	Основные понятия теории информационной безопасности	ОПК-4, ПК-18	Тест
3.	Программно-технические методы защиты	ОПК-4, ПК-18	Тест
4.	Криптографические методы защиты	ОПК-4, ПК-18	Тест
5.	Организационно правовые методы информационной безопасности	ОПК-4, ПК-18	Тест
6.	Роль стандартов в обеспечении информационной безопасности	ОПК-4, ПК-18	Тест

## **6.2. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ**

### **6.2.1. Экзамен**

Билеты для проведения экзамена формируются на основе теоретических вопросов и практических заданий. Билет содержит два теоретических вопроса и одно практическое задание.

*а) Типовые вопросы к эзачету*

#### **Тема 1. Введение в предмет. Угрозы информационной безопасности.**

1. Что называется информационной безопасностью?
2. Какие данные называются критическими?
3. Какие вы знаете признаки компьютерных преступлений в интернет технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений?
4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать?
5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности?

#### **Тема 2. Основные понятия теории информационной безопасности.**

6. Перечислите меры защиты информационной безопасности.
7. Какие меры предпринимают по защите целостности информации?
8. Какие меры предпринимают по защите системных программ?
9. Дублирование информации и его классы.
10. Перечислите позиции административного уровня.
11. Назовите цель ОНРВ и его основные положения?

#### **Тема 3. Программно-технические методы защиты.**

12. Что такое межсетевой экран и какая у него роль в защите.
13. Законодательная основа информационной безопасности, статьи и пр.
14. Что такое политика безопасности на административном уровне?
15. Основные принципы защиты информации на административном уровне?
16. Средства Разграничения доступа.
17. Что такое CGI процедуры, их назначения?
18. Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами?
19. Как осуществляется защита WEB-серверов?

#### **Тема 4. Криптографические методы защиты.**

20. Криптография и криптоанализ. Назначение криптографии.
21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики.
22. Симметричная и асимметричная методология шифрования.
23. Криптографические средства защиты.
24. Квантовая криптография и ККС.

#### **Тема 5. Организационно-правовые методы информационной безопасности.**

25. Чем определяется концепция обеспечения безопасности АСОИ.
26. В чем состоит избирательная политика безопасности способом управления доступом.
27. Организационные меры безопасности АСОИ.
28. Матрица доступа в АСОИ.
29. Полномочное управление доступом.
30. Избирательное управление доступом.

#### **Тема 6. Роль стандартов в обеспечении информационной безопасности.**

31. Что такое универсальная операционная система?
32. Что такое компьютерный вирус.
33. Полиморфные вирусы.
34. Суррогатные платежные средства.
35. Файловые вирусы и алгоритм их работы.
36. Особенность макровирусов.

*б) Типовые практические задания на зачете*

*Задание 1.* Для одноалфавитного метода с задаваемым смещением выполнить шифрование с произвольным смещением.

*Задание 2.* Для одноалфавитного метода с задаваемым смещением выполнить дешифрование зашифрованный шифром Цезаря текст.

*Задание 3.* Проверить на простоту два произвольных целых числа разрядностью 5.

*Задание 4.* Задан интервал вида  $[x, x + L]$ . Вычислить количество  $\Pi(x, L)$  простых чисел в интервале и сравнить с величиной  $L/\ln(x)$ . При каких условиях  $\Pi(x, L)/L$  близко к  $1/\ln(x)$  при заданных  $x = 2000, L = 500$ , количество простых чисел для деления 5-15, количество оснований 1-2?

*Задание 5.* Найти в интервале  $(1000, 1000 + 300)$  все простые числа. Пусть  $L(i)$  - разность между двумя соседними простыми числами. Построить гистограмму для  $L(i)$ . Вычислить выборочное среднее  $L_{\text{сред}}$ . Сравнить с величиной  $\ln(x)$ , где  $x$  - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований 1-3.

*Задание 6.* Для заданного набора чисел  $\{k\}$  оценить относительную погрешность формулы для  $k$ -го простого числа:  
 $p(k) = k/\ln(k), k = \{10, 15, 20, 30, 35\}$ .

*Задание 7.* В интервале  $(500, 500 + 200)$  построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые  $k$  простых. Расчет производится для всех  $k \leq 10$ .

*в) Критерии оценивания компетенций (результатов)*

Уровень сформированности компетенций оценивается по результатам ответов на вопросы и решения практической задачи.

Критерием оценивания ответов на теоретические вопросы к зачету является полнота знаний теоретического материала в области информационной безопасности в профессиональной деятельности, умение излагать материал, отстаивать свою точку зрения, приводить практические примеры используемых в практике стандартов и технических средств информационной безопасности.

Критерием оценивания результатов решения практического задания являются умения применять знания криптографических алгоритмов для решения практических задач.

### **6.2.2 Тест**

а) критерии оценивания компетенций (результатов): *зачтено / незачтено*

б) описание шкалы оценивания

«Зачтено» - выставляется студенту, давшему 60 % или более правильных ответов.

«Незачтено» - выставляется студенту, давшему менее 60 % правильных ответов.

в) примерные вопросы тестов по темам

### **Вариант 1**

#### **Тема 1. Введение в предмет. Угрозы информационной безопасности.**

1. Перечислите четыре уровня защиты компьютерных и информационных ресурсов?

А. Предотвращение, обнаружение, ликвидация, восстановление.

Б. Предотвращение, описание, ликвидация, восстановление.

В. Предотвращение, обнаружение, ограничение, восстановление.

2. Что называют критическими данными?

А. Данные, которые требуют сохранения из-за вероятности нанесения умышленного ущерба.

Б. Данные, которые требуют защиты из-за вероятности нанесения ущерба, если

произойдет случайное или умышленное раскрытие данных.

В. Данные, которые требуют уничтожения из-за вероятности нанесения случайного ущерба при раскрытии данных.

3. *Основные меры защиты информационной безопасности?*

А. Идентификация, аутентификация.

Б. Паролирование, кодирование.

В. Авторизация, дублирование.

4. *Что понимается под надежностью компьютерных систем?*

А. Способность системы восстанавливать информацию при отказах отдельных устройств.

Б. Отказ системы на вход неидентифицированного пользователя.

В. Свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации.

5. *Что такое идентификатор пользователя?*

А. Номер пользователя в журнале учетных записей.

Б. Уникальная информация, позволяющая различать индивидуальных пользователей.

В. Пароль для входа в систему.

## **Тема 2. Основные понятия теории информационной безопасности.**

6. *Способы доступа к данным:*

А. Прямой, обратный.

Б. Параллельный, прямой.

В. Последовательный, прямой.

7. *Что такое межсетевой экран?*

А. Средство разграничения доступа, служащие для защиты от внешних угроз.

Б. Средство разграничения доступа, служащее для защиты от внешних угроз и угроз со стороны пользователей других сегментов корпоративных сетей.

В. Средство защиты от угроз со стороны пользователей других сегментов корпоративных сетей.

8. *Основные подходы к созданию отказоустойчивых систем:*

А. Помехоустойчивое кодирование информации, параллельный доступ к информации.

Б. Простое резервирование, помехоустойчивое кодирование информации, создание адаптивных систем.

В. Создание адаптивных систем, зеркальное дублирование информации, резервирование.

9. *По времени восстановления информации методы дублирования делятся на:*

А. Оперативные, неоперативные.

Б. Статические, динамические.

В. Кратковременные, долговременные.

10. *Что такое отказоустойчивость компьютерных систем?*

А. Свойство компьютерной системы сохранять работоспособность при отказах отдельных устройств, блоков, схем.

Б. Способность компьютерной системы сохранять информацию при сбоях.

В. Возможность дублирования информации на съемные носители.

## **Тема 3. Программно-технические методы защиты.**

11. Средства, используемые для блокировки ошибочных операций:

- А. Программные, аппаратные.
- Б. Физические, технические.
- В. Технические, аппаратно-программные.

12. Что такое аутентификация пользователей?

- А. Метод, применяемый для подтверждения и проверки пользователей.
- Б. Процедура, необходимая для входа в компьютерную систему.
- В. Процесс входа в компьютерную систему.

13. Что такое информационная безопасность?

- А. Меры по защите информации от несанкционированного доступа.
- Б. Меры по восстановлению информации, ограничению доступа, обнаружению ошибок, предотвращению преступлений.
- В. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

14. Что такое криптография?

- А. Наука о способах преобразования информации с целью защиты от несанкционированного доступа.
- Б. Вид шифрования и кодировки информации.
- В. Метод защиты информации.

15. Для чего используются CGI-процедуры?

- А. Для статического отображения HTML-документов.
- Б. Для распределения прав доступа к серверу.
- В. Для динамического порождения HTML-документов.

#### **Тема 4. Криптографические методы защиты.**

16. Уровни защиты информации в Intranet:

- А. Морально-этический, программно-технический, физический.
- Б. Административный, процедурный, законодательный.
- В. Протокольный, межсетевой, уровень фильтрации доступа.

17. Что такое криптология?

- А. Шифрование/ дешифрование информации.
- Б. Наука, состоящая из криптографии и криптоанализа.
- В. Применение криптографии на практике.

18. Какая кампания первой предложила технологию, позволяющую использовать пластиковые карты для расчетов в сети?

- А. Visa.
- Б. Master Card.
- В. Cyber Cash.

19. Что такое карта памяти?

- А. Пластиковая карта с магнитной полосой с обратной стороны, которая считывается специальным устройством.
- Б. Карта со встроенной микросхемой, содержащей устройство для записи/считывания информации.
- В. Специальные цифровые купоны и жетоны.

#### **Тема 5. Организационно-правовые методы информационной безопасности.**

20. Что такое вскрытие шифра?

- А. Процесс получения защищаемой информации.
- Б. Процесс получения защищаемой информации из зашифрованного сообщения со знанием примененного шифра.
- В. Процесс получения защищаемой информации из зашифрованного сообщения без предварительного знания примененного шифра.

21. *Какие протоколы используются для квантово-криптографических систем?*

А. Протокол первичной квантовой передачи, протокол исправления ошибок в битовых последовательностях, протокол оценки утечки к злоумышленнику информации о ключе, протокол усиления секретности и формирования итогового ключа.

Б. Протокол вторичной квантовой передачи, протокол исправления ошибок в данных, протокол оценки утечки информации, протокол уменьшения секретности ключа.

В. Протокол квантовой передачи, протокол битовых последовательностей, протокол оценки утечки к злоумышленнику информации о ключе, протокол формирования итогового ключа.

22. *Методологии шифрования:*

А. Симметричная, асимметричная.

Б. Прямая, зеркальная.

В. Открытая, закрытая.

23. *Для чего используется электронная подпись?*

А. Позволяет проверять целостность данных, но не обеспечивает их конфиденциальность.

Б. Позволяет проверять целостность данных, и обеспечивает их конфиденциальность.

В. Не позволяет проверять целостность данных, но обеспечивает их конфиденциальность.

24. *Что такое компьютерный вирус?*

А. Небольшие исполняемые программы, обладающие свойством распространения и репликации в компьютерной системе.

Б. Информационные системы, обладающие свойством распространения и самовоспроизведения.

В. Программные комплексы, изменяющие или уничтожающие программное обеспечение, не обладающие свойством самовоспроизведения.

25. *По способу заражения среды обитания компьютерные вирусы делятся на:*

А. Резидентные, нерезидентные.

Б. Целостные, частичные.

В. Оперативные, неоперативные.

**Тема 6. Роль стандартов в обеспечении информационной безопасности.**

26. *По степени опасности для информационных ресурсов компьютерные вирусы делятся на:*

А. Безопасные, частично опасные, опасные.

Б. Безвредные, частично опасные, очень опасные.

В. Безвредные, опасные, очень опасные.

27. *Что такое макровирус?*

А. Вредительская программа, имеющая большую среду обитания.

Б. Вредительская программа, написанная на макроязыках, встроенных в текстовые редакторы, электронные таблицы и др.

В. Вредительская программа, заражающая программно-аппаратные средства.

28. *Какие методы из перечисленных являются методами обнаружения вирусов?*

А. Сканирование, вакцинирование программ, обнаружение изменений.

Б. Сканирование, шифрование, криптоанализ.

В. Эвристический анализ, криптозащита, аутентификация.

29. Для каких целей применяют антивирусные средства?

А. Для создания, копирования, изменения вирусов.

Б. Для обнаружения, блокирования работы вирусов, устранения последствий воздействия вирусов.

В. Для обнаружения и удаления вирусов.

30. Что включают организационные методы защиты информации?

А. Меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации компьютерных систем для обеспечения заданного уровня безопасности информации.

Б. Меры, мероприятия и действия, которые должен осуществлять персонал в процессе эксплуатации компьютерных систем.

В. Действия, которые должен осуществлять разработчик в процессе создания компьютерных систем для обеспечения заданного уровня безопасности информации.

### **6.2.3 Контрольная работа**

*а) Тематика контрольных работ*

**Тема 1. Введение в предмет. Угрозы информационной безопасности.**

1. Политика информационной безопасности предприятия.
2. Нормативно-правовая база обеспечения информационной безопасности предприятия.
3. Содержание основных законов Российской Федерации в сфере компьютерного права.
4. Законодательная база РФ по вопросам защиты информации.
5. Комплексный подход к обеспечению информационной безопасности.

**Тема 2. Основные понятия теории информационной безопасности.**

1. Законодательные и нормативные акты РФ о предпринимательской деятельности.
2. Машинное представление информации.
3. Виды и формы представления информации.
4. Информация как объект права собственности.
5. Информация как коммерческая тайна.
6. Информация как рыночный продукт.
7. Элементы и объекты защиты в АС.

**Тема 3. Программно-технические методы защиты.**

1. Основные виды вирусов и схемы их функционирования.
2. Обнаружение вирусов и меры по защите и профилактике
3. Основные меры защиты от вирусов.
4. Программно-технические меры обеспечения информационной безопасности.
5. Обеспечение информационной безопасности средствами Windows 7.

**Тема 4. Криптографические методы защиты.**

1. Безопасное хранение данных на основе шифрования.
2. Американский стандарт шифрования данных DES.
3. Стандарт шифрования данных ГОСТ 28147-89.

4. Система цифровой телефонии.
5. Системы шифрования с открытыми ключами.

**Тема 5. Организационно-правовые методы информационной безопасности.**

1. Цифровые подписи на основе шифросистем с открытыми ключами.
2. Комплексный подход к обеспечению информационной безопасности:
3. Механические системы защиты

**Тема 6. Роль стандартов в обеспечении информационной безопасности.**

1. Политика информационной безопасности предприятия.
2. Нормативно-правовая база обеспечения информационной безопасности предприятия.
3. Содержание основных законов Российской Федерации в сфере компьютерного права.
4. Законодательная база РФ по вопросам защиты информации.
5. Комплексный подход к обеспечению информационной безопасности.
6. Законодательные и нормативные акты РФ о предпринимательской деятельности.

*б) критерии оценивания*

Критериями оценивания доклада являются полнота раскрытия темы, степень ее проработанности, последовательность изложения материала; умения студента самостоятельно работать с литературой и информационно-электронными ресурсами, аргументированно и ясно строить речь, эффективно и наглядно представлять содержание результатов своей работы, а также владения навыками дискуссии и публичной защиты результатов своих исследований.

*в) описание шкалы оценивания*

Контрольные работы оцениваются по шкале «зачтено» / «незачтено».

«Зачтено» выставляется в случае, если студент свободно излагает материал по заданному вопросу, опираясь при этом на литературные и другие дополнительные источники, отвечает на дополнительные уточняющие вопросы преподавателя и аудитории студентов, приводит практические примеры, аргументированно отстаивает свою точку зрения; во время доклада использует раздаточный материал и (или) презентацию.

«Незачтено» выставляется в случае, если в изложении наблюдаются значительные пробелы в знании материала и (или) студент не отвечает на дополнительные уточняющие вопросы и (или) не использует иллюстративный материал.

**6.3. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ**

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1.	Отчет по практической работе	Отчеты принимаются индивидуально у каждого студента в течение лабораторного занятия. Проводится также собеседование, в ходе которого можно проверить знания терминологии, основных методов информацион-	Комплект заданий к лабораторным работам

		ной безопасности, а также умения студента представлять результаты своей работы и аргументированно отстаивать свою точку зрения.	
2.	Тест	Тестирование проводится на бумажных носителях. Время на выполнение тестовых заданий составляет 15 минут. Результаты тестирования позволяют оценить уровень теоретической подготовленности студента.	Тестовые задания

**Текущий контроль** теоретических знаний осуществляется в процессе проведения всех видов занятий.

**Промежуточный контроль** теоретических знаний осуществляется путем тестового опроса по блокам тем, практических умений путем выполнения аудиторной самостоятельной работы.

При промежуточном и текущем контроле оценивается правильность ответов и решения заданий.

Итоговый контроль осуществляется на экзамене.

## 7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

### а) Основная литература

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. Режим доступа: <http://www.znanium.com/bookread.php?book=405000>
2. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учебник / В. Ф. Шаньгин. – Электронные текстовые данные. –Москва : ДМК Пресс, 2012.- Режим доступа: [http://e.lanbook.com/books/element.php?pl1\\_cid=25&pl1\\_id=3032](http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3032)

### б) Дополнительная литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
6. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинкова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.
7. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.

8. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

## 8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» (ДАЛЕЕ - СЕТЬ «ИНТЕРНЕТ»), НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- Новая электронная библиотека – [www.newlibrary.ru](http://www.newlibrary.ru)
- Российское образование (федеральный портал) – [www.edu.ru](http://www.edu.ru)
- Нехудожественная библиотека – [www.nehudlit.ru](http://www.nehudlit.ru)
- Научная электронная библиотека [www.e-library.ru](http://www.e-library.ru)
- Университетская информационная система [www.uisrussia.ru](http://www.uisrussia.ru)

## 9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом (раздел 7 рабочей программы).
Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций и рекомендуемую литературу.

## 10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ), ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ (ПРИ НЕОБХОДИМОСТИ)

№	Наименование раздела дисциплины	Информационные технологии
1	Введение в предмет. Угрозы информационной безопасности	MS Power Point, MS Word
2	Основные понятия теории информационной безопасности	MS Power Point, MS Word
3	Программно-технические методы защиты	MS Visio, Delphi, MS Visual Studio
4	Криптографические методы защиты	MS Visio, Delphi, MS Visual Studio
5	Организационно-правовые методы информационной без-	MS Power Point, MS Excel, MS

	опасности	Word
6	Роль стандартов в обеспечении информационной безопасности	MS Excel, MS Power Point

## 11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для обеспечения высокого класса преподавания дисциплины «Методы и средства защиты информации», а также для более эффективного усвоения материала студентами рекомендуется применение следующих технических средств:

- компьютер, проектор и экран для демонстрации лекции в режиме Power Point;
- компьютерный класс для проведения практических занятий;
- доступ в Интернет для студентов во время проведения практических занятий.

## 12. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

В соответствии с ФГОС ВПО по направлению подготовки 09.03.03 Прикладная информатика «Реализация компетентного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся». Проведение занятий в интерактивной форме предусмотрено в рамках данной дисциплины в объеме 12 часов для студентов очной формы обучения

Тема	Вид занятия/содержание занятия	Часы	Технология
Тема 2. Основные понятия теории информационной безопасности	<b>Практическое занятие.</b> Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль	4	Анализ конкретной ситуации: обучающиеся должны проанализировать предложенную конфигурацию защиты, определить уязвимые места и разработать методику их ликвидации.
Тема 3. Программно-технические методы защиты	<b>Практическое занятие.</b> Методы современной криптографии на примере программирования одного из предложенных алгоритмов	4	Анализ конкретной ситуации: обучающиеся должны проанализировать предложенную конфигурацию защиты и предложить набор программно-технических средств для реализации информационной безопасности предприятия
Тема 6. Роль стандартов в обеспечении информационной безопасности	<b>Практическое занятие.</b> Составление документа «Политика безопасности»	4	Анализ конкретной ситуации: обучающиеся должны проанализировать деятельность предложенного предприятия и оформить документ «Политика безопасности»

Составитель: Антонов А.В., старший преподаватель кафедры информационных систем и управления