НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГУМАНИТАРНЫЙ
УНИВЕРСИТЕТ ПРОФСОЮЗОВ»

Кафедра Информатики и математики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность

Основная профессиональная образовательная программа
высшего образования программы бакалавриата
по направлению

09.03.03 «Прикладная информатика»

Профиль подготовки «Прикладная информатика в экономике»

Квалификация:
Бакалавр

Согласовано:
Руководитель ОПОП по направлению 09.03.03 – «Прикладная информатика» Профиль «Прикладная информатика в экономике»
_____/Путькина Л.В.

Рассмотрена и утверждена на заседании кафедры

«01» июня 2020 г., протокол № 10

Зав. кафедрой _____/Путькина Л.В.
Рекомендована решением
Методического совета

«15» июня 2020 г., протокол № 10

Секретарь МС _____/Волкова А.М.

Авторы-разработчики:

_____/Мокрый В.Ю.

Санкт-Петербург

СТРУКТУРА

1.Цель и задачи освоения дисциплины:

Целью освоения **дисциплины «Информационная безопасность»** является изучение различных видов информационных угроз (включая компьютерные вирусы) и методов противодействия им; основных принципов и стандартов; различных профилей информационной безопасности; видов политики обеспечения информационной безопасности.

Основные **задачи дисциплины**:

– формирование навыков безопасной работы с информацией, включая работу в локальных и глобальных компьютерных сетях, в средах различных ОС; навыков практической реализации методов информационной защиты, разработки систем защиты информации (СЗИ), включая требования к таким системам.

– формирование представления об этапах развития безопасности информационных систем;

– изучение основных тенденций развития современных типов операционных систем;

– формирование навыков обеспечения безопасности веб-приложений.

2.Место дисциплины в структуре ОПОП:

Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ разделов данной дисциплины, необходимых для изучения обеспечиваемых дисциплин			
		1	2	3	4
1.	Информационные системы и технологии	+	+	+	+
2.	Правовая защита интеллектуальной собственности	+	+	+	+
3.	Проектный практикум	+	+		
4.	Маркетинг			+	+

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций с установленными к ним индикаторами:

Компетенции и индикаторы их достижения

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.

4. Тематический план изучения дисциплины
См. Приложение

5. Содержание разделов и тем дисциплины

РАЗДЕЛ 1 (Модуль 1). Введение

Тема 1. Социальные, политологические и правовые аспекты, виды безопасности
Понятия информационной безопасности, информационных угроз. Законодательство в области защиты информации.

Тема 2. Сетевые протоколы и модели взаимодействия открытых систем
Стандарты взаимодействия открытых систем и их роли в обеспечении информационной безопасности. Архитектуры и топологии открытых систем**.** Цели использования сетевых технологий и принципы построения сетевых программных интерфейсов.

РАЗДЕЛ 2 (Модуль 2). Защита вычислительных систем

Тема 3. Тенденции развития безопасности операционных систем. Представление об этапах развития безопасности операционных систем. Основные тенденции развития основных типов операционных систем. Примеры сетей. Продукция компании Микрософт и UNIX-подобных операционных систем.

Тема 4. Средства и алгоритмы управления процессами, и памятью ОС. Плоская модель памяти и её использование в программировании. Механизм защиты процессора Intel: схемы управления памятью и защита по привилегиям являются основой для обеспечения безопасности операционных систем.

РАЗДЕЛ 3 (Модуль 3). Защита клиентских и серверных приложений

Тема 5. Безопасность клиентских приложений. Использование методов объекта Document и объекта Response. Методы объекта Document и объекта Response. Объект Request и области его применения. Подходы к хранению в базе данных информации о пользователе, минимизация размеров таблицы базы, отслеживание информации о каждом отдельном пользователе и затратах ресурсов сервера. Технология обработки событий в ASP и ее применение для целей обеспечения информационной безопасности

Тема 6. Клиентский и серверный скрипт с позиций информационной безопасности. Клиентский и серверный скрипт с позиций информационной безопасности. Технологии передачи информации, методы защиты информации при использовании клиентский и серверный скриптов. Технология PHP и использования баз данных MySQL для размещения учетной информации.

РАЗДЕЛ 4 (Модуль 4). Подходы к защите информации

Тема 7. Каналы утечки информации. Способы несанкционированного доступа к конфиденциальной информации. Вопросы администрирования компьютерных сетей. Настройки домена и его безопасность. Технологии потенциально возможных злоумышленных действий при организации обработки данных. Методологические подходы к оценке уязвимости информации

Тема 8. Классы задач защиты. Стратегии защиты информации. Использование задач защиты информации в сопоставлении с видами угроз. Характер происхождения угроз. Вопросы систематизации каналов несанкционированного получения информации. Причины нарушения целостности информации. Понятие информационной инфекции.

Тема 9. Понятие уязвимости информации, подходы к оценке уязвимости информации. Обобщенная схема злонамеренных действий. Построение модели поведения нарушителя

информационных систем. Причины нарушения целостности информации. Функции защиты информации и классы задач защиты информации. Стратегии защиты информации.

Тема 10. Криптографическая защита информации в Интернете. Понятие Симметричного и асимметричного шифрования. Вопросы, связанные с формированием требований к криптосистемам Алгоритмы шифрования и криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. Изучение методов криптоанализа и технологий атак на криптосистемы. Юридические аспекты использования цифровой подписи и организационные аспекты ее применения. Защита информации в Интернете с технологиями WAP (Wireless Application Protocol).

6. План подгрупповых (лабораторных) занятий

№ п/п	Наименование темы дисциплины	Наименование и содержание подгрупповых (лабораторных) занятий, литература для подготовки к занятиям	Формируемые компетенции	Формы контроля усвоения знаний
1.	Социальные, политологические и правовые аспекты, виды безопасности	Понятия информационной безопасности, информационных угроз. Законодательство в области защиты информации. Задание для самостоятельной работы: прежде всего, следует ознакомиться с концепциями построения информационных систем – этапы развития, примеры, классификации и структура информационной системы. Ознакомление с угрозами безопасности информации охватывает вопросы причин и источников угроз безопасности, реагирование на инциденты, управление конфигурациями, пользователями, рисками, инструментарий информационной безопасности. При самостоятельном изучении данного раздела целесообразно ознакомиться с материалом, представленным в списке литературы. **Задания** 1) Проанализировать существующие взгляды на понятие «Информационная безопасность», выделить ключевые слова и составить схему взаимосвязей между ними. 2) Выделить взаимосвязи между	ОПК-3	Опрос

		понятиями «Информационная безопасность» и «Компьютерная безопасность». 3) Привести примеры социальных, политологических и правовых аспектов информационной безопасности. Литература: 1-4.		
2.	Сетевые протоколы и модели взаимодействия открытых систем	Стандарты взаимодействия открытых систем и их роли в обеспечении информационной безопасности. Архитектуры и топологии открытых систем**.** **Задания** 1) Описать основные характеристики компьютерной сети и её сервисов. 2) Привести особенности основных протоколов и области их применения. 3) Указать угрозы защищённости компьютера пользователя в соответствии с уровнями модели открытых систем. Литература: 1-4.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения
3.	Тенденции развития безопасности операционных систем	Представление об этапах развития безопасности операционных систем. Основные тенденции развития основных типов операционных систем. Примеры сетей. Продукция компании Микрософт и UNIX-подобных операционных систем. **Задания** 1) Выделить угрозы безопасности компьютерных систем. 2) Выделить угрозы безопасности сетевых и локальных версий операционных систем. 3) Опишите основные средства, применяемые для защиты операционных систем. Литература: 1-4.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения
4.	Средства и алгоритмы управления процессами, и памятью ОС	Плоская модель памяти и её использование в программировании. Механизм защиты процессора Intel: схемы управления памятью и защита по	ОПК-3	Опрос, проверка заданий для самостоятельного

		привилегиям являются основой для обеспечения безопасности операционных систем. **Задания** 1) Привести описание моделей организации памяти в вычислительных системах. 2) Привести этапы развития средств управления памятью и процессами в операционной системе. 3) Привести особенности существующих средств управления процессами и памятью операционной системе. Литература: 1-4.		выполнения
5.	Безопасность клиентских приложений	Использование методов объекта Document и объекта Response. Изучите методы объекта Document и объекта Response. Объект Request и области его применения. Задание для самостоятельной работы: Особое внимание нужно уделить хранению в базе данных информации о пользователе, а также минимизации размеров таблицы базы и отслеживание информации о каждом отдельном пользователе и затратах ресурсов сервера. Студенту следует изучить технологию обработки событий в ASP и ее применения для целей обеспечения информационной безопасности. **Задания** 1) Укажите отличие между программным обеспечением, установленным на сервере и клиентскими приложениями. 2) Приведите примеры возникновения угроз безопасности клиентских приложений. 3) Приведите примеры информационных систем, разработанных по архитектуре клиент-сервер. Литература: 1-4.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения
6.	Клиентский и	Клиентский и серверный скрипт с	ОПК-3	Опрос,

	серверный скрипт с позиций информационной безопасности	позиций информационной безопасности. **Задания** 1) Приведите особенности языков программирования с помощью сценариев. 2) Укажите отличия между скриптами и исполняемыми файлами. 3) Приведите примеры программ на языке Javascript и их назначение. Литература: 1-4.		проверка заданий для самостоятельного выполнения
7.	Каналы утечки информации. Способы несанкционированного доступа к конфиденциальной информации	Вопросы администрирования компьютерных сетей. Настройки домена и его безопасность. Технологии потенциально возможных злоумышленных действий при организации обработки данных. **Задания** 1) Приведите примеры средств, позволяющих получить несанкционированный доступ к информации. Укажите статьи законов и актов, которые устанавливают ответственность за такие правонарушения. 2) Приведите примеры каналов утечек информации. 3) Приведите возможные меры, которые должны быть предприняты в организации для защиты от угроз защищённости конфиденциальной информации. Литература: 1-4.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения
8.	Классы задач защиты. Стратегии защиты информации	Использование задач защиты информации в сопоставлении с видами угроз. **Задания** 1) Приведите примеры организационных, технических и инженерных мер по защите информации в различных организациях. 2) Опишите особенности программ, которые могут быть использованы для защиты информации.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения

		3) Приведите примеры аппаратных средств, предназначенных для защиты информации. Литература: 1-4.		
9.	Понятие уязвимости информации, подходы к оценке уязвимости информации	Обобщенная схема злонамеренных действий. Построение модели поведения нарушителя информационных систем. Причины нарушения целостности информации. **Задания** 1) Приведите примеры организационных, технических и инженерных мер по защите информации в различных организациях. 2) Опишите особенности программ, которые могут быть использованы для защиты информации. 3) Приведите примеры аппаратных средств, предназначенных для защиты информации. Литература: 1-4.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения
10.	Криптографическая защита информации в Интернете	Понятие Симметричного и асимметричного шифрования. Вопросы, связанные с формированием требований к криптосистемам Алгоритмы шифрования и криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. **Задания** 1) Укажите классификацию алгоритмов шифрования. 2) Задания №2. Опишите основные сервисы и программы, позволяющие шифровать информацию. 3) Задания №3. Приведите примеры инструментов для защиты информации на корпоративных порталах. Литература: 1-4.	ОПК-3	Опрос, проверка заданий для самостоятельного выполнения

7. Образовательные технологии

При проведении учебных занятий по дисциплине для успешного освоения применяются различные образовательные технологии, которые обеспечивают развитие навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

Методы / Формы	Лекции (Л)	Подгрупповые занятия (П)
Диалого-дискуссионное обсуждение проблем	+	+
Работа в команде		+
Поисковый метод	+	+
Проектный метод		+
Исследовательский метод		+

8. План самостоятельной работы студентов

№ п/п	Содержание самостоятельной работы студентов	Формируемые компетенции	Форма отчётности студента
1	Изучение литературы по темам дисциплины	ОПК-3	Составление обзора литературы для подготовки к экзамену
2	Выполнение заданий для самостоятельной работы	ОПК-3	Файлы с заданиями
3	Изучение теоретического материала дисциплины	ОПК-3	Экзамен

9. Контроль знаний по дисциплине

По дисциплине предусмотрен текущий и промежуточная аттестация.

Текущий контроль успеваемости студента – одна из составляющих оценки качества усвоения образовательных программ. Текущий контроль проводится в течение семестра

Промежуточная аттестация проводится по окончании изучения дисциплины в виде экзамена.

Вопросы к промежуточной аттестации сформулированы в **Оценочных и методических материалах**.

10. Учебно-методическое и информационное обеспечение дисциплины:

а) Основная литература

1. Васильева И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/433610

2. Внуков А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/444046

3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин,

А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/437163

4. Хлебников А. А. Информационные технологии : учебник / Хлебников А.А. — Москва : КноРус, 2018. — Режим доступа: https://book.ru/book/927689

б) Дополнительная литература:

1. Внуков А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — Режим доступа: https://urait.ru/bcode/414083

2. Воронцова С. В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок): монография / С. В. Воронцова. — М. : КноРус, 2017. — Режим доступа: http://www.book.ru/book/921936

3. Казарин О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/441287

4. Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/447581

5. Путькина Л. В. Информатика и математика для гуманитарных вузов : учебное пособие / Л. В. Путькина, Т. Г. Пискунова, Т. Б. Антипова ; СПб Гуманит. ун-т профсоюзов. — СПб. : Изд-во СПбГУП, 2014. — Режим доступа**:** http://library.gup.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=108&task=set_static_req&sys_code=32/39/П 90-168317&bns_string=IBIS

6. Советов Б. Я. Информационные технологии : учебник для прикладного бакалавриата / Б. Я. Советов, В. В. Цехановский. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/431946

7. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/433420

8. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019. — Режим доступа: https://urait.ru/bcode/434104

в) Периодические издания

1. Журнал «Вестник Томского государственного педагогического университета» [Электронный ресурс]. Режим доступа: https://vestnik.tspu.edu.ru/

г) Лицензионное программное обеспечение

1. Семейство программ Microsoft Office Standart Russian (Включает набор продуктов: Word, Excel, PowerPoint, Publisher, Outlook);
2. Mirapolis Virtual Room;
3. Антиплагиат;
4. КонсультантПлюс
5. Project Expert 7
6. Prime Expert
7. FineModel Expert

8. Обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде СПбГУП.

д) Современные профессиональные базы данных и информационные справочные системы

1. Официальный сайт СПбГУП: http://www.gup.ru/
2. Электронно-библиотечная система СПбГУП http://library.gup.ru
3. Системы поддержки самостоятельной работы СПбГУП: http://edu.gup.ru/
4. Справочная правовая система «КонсультантПлюс» (версия ПРОФ), установленная в Университете
5. Российское образование http://www.edu.ru/
6. Единое окно доступа к образовательным ресурсам http://window.edu.ru/
7. Электронно-библиотечная система http://e.lanbook.com/

11. Материально-техническое обеспечение дисциплины

Аудиторный фонд с демонстрационным оборудованием и техническими средствами обучения, учебно-наглядные пособия и методические ресурсы кафедры, фонды Научной библиотеки.

Изучение дисциплины инвалидами и обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья обучающихся.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

1. Методические рекомендации по организации самостоятельной работы студентов

Самостоятельная работа в высшем учебном заведении является важной организационной формой индивидуального изучения студентами программного материала. Эти слова особенно актуальны в наше время, когда в педагогике высококвалифицированных специалистов широко используется дистанционное обучение, предполагающее значительную самостоятельную работу студента на основе рекомендаций преподавателя.

2. Методические рекомендации по подготовке к практическим (подгрупповым) занятиям

Подгрупповые занятия – важная форма учебного процесса. Они способствуют закреплению и углублению знаний, полученных студентами на лекциях и в результате самостоятельной работы над научной и учебной литературой и нормативными источниками. Они призваны развивать самостоятельность мышления, умение делать выводы, связывать теоретические положения с практикой, формировать профессиональное правовое сознание будущих бакалавров. На занятиях вырабатываются необходимые каждому юристу навыки и умения публично выступать, логика доказывания, культура профессиональной речи. Кроме того, семинары – это средство контроля преподавателей за самостоятельной работой студентов, они непосредственно влияют на уровень подготовки к итоговым формам отчетности – зачетам и экзаменам. В выступлении на семинарском занятии должны содержаться следующие элементы:

- четкое формулирование соответствующего теоретического положения в виде развернутого определения;
- приведение и раскрытие основных черт, признаков, значения и роли изучаемого явления или доказательства определенного теоретического положения;
- подкрепление теоретических положений конкретными фактами.

Для качественного и эффективного изучения дисциплины необходимо овладение навыками работы с книгой, воспитание в себе стремления и привычки получать новые знания из научной и иной специальной литературы. Без этих качеств не может быть настоящего специалиста ни в одной области деятельности.

Читать и изучать, следует, прежде всего, то, что рекомендуется к каждой теме программой, планом семинарских занятий, перечнем рекомендуемой литературы.

Когда студент приступает к самостоятельной работе, то он должен проявить инициативу в поиске специальных источников. Многие новейшие научные положения появляются, прежде всего, в статях, опубликованных в журналах.

Надо иметь в виду, что в каждом последнем номере издаваемых журналов публикуется библиография всех статей, напечатанных за год, это облегчает поиск нужных научных публикаций.

Работа с научной литературой, в конечном счете, должна привести к выработке у студента умения самостоятельно размышлять о предмете и объекте изучения, которое должно проявляться:

- в ясном и отчетливом понимании основных понятий и суждений, содержащихся в публикации, разработке доказательств, подтверждающих истинность тех или иных положений;

- в понимании студентами обоснованности и целесообразности, приводимых в книге и статье примеров, поясняющих доказательства и выводы автора. При этом будет уместно, если студент самостоятельно приведет дополнительные примеры к этим выводам;
- в отделении основных положений от дополнительных, второстепенных сведений;
- в способности студента критически разобраться в содержании публикации, определить свое отношение к ней в целом, дать ей общую оценку, характеристику.

3. Методические рекомендации по написанию контрольных работ

Важнейшей формой учебной отчётности студента является **контрольная работа**.

Выполнение контрольной работы является промежуточной формой отчётности по изучаемой дисциплине и преследует цель лишь оценить способность студента к самостоятельному поиску источников, формированию содержания и его письменного изложения по указанной проблеме. Это важная составляющая изучения дисциплины, а также эффективная форма контроля знаний. При заочном обучении она выступает как обязательная, основная форма самостоятельной работы. В контрольной работе (в соответствии с учебным планом) студент обязан самостоятельно глубоко разобраться в изучаемых проблемах, усвоить суть темы, уяснить её содержание и только затем письменно представить свою отчётную работу.

Выполнение контрольной работы является одним из условий допуска студента к сдаче экзамена. Работа должна соответствовать установленным требованиям, то есть в ней должны быть раскрыты все проблемы, определённые темой. Для этого студент обязан самостоятельно проанализировать первоисточники и дать исчерпывающие ответы на вопросы темы. Контрольная работа – серьёзное учебное задание, и чтобы написать её как следует, необходимо использовать те первоисточники и учебные пособия, которые позволяют полнее разобраться в проблеме. Студент должен регулярно работать в университетской и городской библиотеке, вдумчиво конспектировать лекции преподавателей.

При написании контрольной работы следует обращать особое внимание на грамотное использование терминологии. При употреблении впервые тех или иных терминов и понятий следует давать их определения либо в самом тексте, либо в сносках.

Приступая к контрольной работе, требуется сначала ознакомиться с имеющейся литературой по теме, изучить первоисточники и составить план. Здесь, в отличие от курсовой работы, план предполагает рассмотрение одной, причём довольно широкой, проблемы, и он может состоять из двух-трёх вопросов. Минимальное количество первоисточников, привлекаемых для написания курсовой работы — пять наименований.

Как правило, контрольные работы по дисциплине сугубо индивидуальны, то есть их тематика персонифицирована. Однако в отдельных случаях темы контрольных работ могут быть адресованы и сразу нескольким, и группе в целом. Таким приёмом преподаватель выявляет степень усвоения какой-то важной учебной проблемы и определяет необходимость проведения дополнительных занятий по какой-либо теме. В настоящее время широко используется методика компьютерного тестирования знаний студентов по дисциплинам, в результате чего появляется возможность быстро проверять знания по наиболее важным темам и объективно оценивать их. Эта форма также может выступать как вид контрольной работы.

В качестве контрольной работы широко применяется самостоятельное изучение монографического исследования по конкретной, крайне важной проблеме, требующей глубокого рассмотрения. Этот вид работы предполагает не простое знакомство с определённым монографическим исследованием, а детальное его изучение. Для этого

студенту важно знать некоторые правила работы с первоисточником, которым для него будет являться монография. Следует выяснить фамилию автора, его имя и отчество, учёную степень и звание, а также что побудило его взяться за изучение данной проблемы; обратить внимание на основные вопросы монографии и их разрешение автором, уметь раскрывать их в ходе собеседования с преподавателем.

Студенту следует письменно (предельно кратко) очертить те вопросы (полностью или частично), которые поставлены автором в монографическом исследовании; при изложении их следует указывать страницы источника.

Задания для написания контрольных работ (для заочной формы обучения)

1. Обзор факторов, механизмов и инструментария информационной безопасности.
2. Информационная безопасность в постиндустриальном и информационном обществе.
3. Информационная безопасность в государственном управлении. Доктрина информационной безопасности Российской Федерации.
4. Информационная безопасность в бизнесе и быту.
5. Служба информационной безопасности в структуре предприятия.
6. Проблемы информационной безопасности малых предприятий.
7. Политика информационной безопасности организации, ее разработка, реализация, модификация.
8. Нормативное обеспечение работы службы информационной безопасности.
9. Исторический обзор развития криптографии, стеганографии, криптоанализа и их основные методы.
10. Обзор методов цифровой потоковой и блочной криптографии.
11. Обзор цифровых блочных шифров DES, ГОСТ 28147-89.
12. Обзор цифровых блочных шифров TEA, IDEA.
13. Конкурс AES и цифровой блочный шифр RIJNDAEL.
14. Конкурс AES и цифровой блочный шифр SERPENT.
15. Конкурс AES и цифровой блочный шифр TWOFISH.
16. Конкурс AES и цифровой блочный шифр RC6.
17. Конкурс AES и цифровой блочный шифр MARS.
18. Обзор технологий асимметричной криптографии и электронной цифровой подписи.
19. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология RSA.
20. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология Рабина.
21. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология Эль Гамаль.
22. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технологии на основе эллиптических кривых.
23. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология Мак-Элиса.
24. Обзор технологий асимметричной криптографии и электронной цифровой подписи, ГОСТ Р 34.10-2001.
25. Криптографические хеш-функции.
26. Обзор возможных атак на информационные системы: локальные атаки; удаленные атаки; атаки на поток данных.
27. Обзор информационной безопасности Windows и Unix-систем, компьютерные вирусы и защита от них.

28. Контроль физического доступа: системы охраны периметра, управления доступом, видеонаблюдения, пожарной сигнализации и др.

29. Сетевая безопасность организации: протоколы сетевой безопасности; антивирусные программы; межсетевые экраны; системы обнаружения атак; технологии VPN и VLAN.

30. Теория открытых систем как теоретическая основа стандартизации, обзор оценочных стандартов и спецификаций информационной безопасности.

31. Стандарты информационной безопасности «Оранжевая книга», «Гостехкомиссия России. Руководящий документ», «Общие критерии» (ГОСТ Р ИСО/МЭК 15408) и их использование в государственном управлении и бизнесе.

32. Спецификации интернет-сообщества по информационной безопасности и их использование в государственном управлении и бизнесе.

Принципы выбора темы работы

Студенты при написании контрольной работы могут выбрать любую из предложенных тем на своё усмотрение.

4. Методические рекомендации по написанию курсовой работы

Курсовая работа учебным планом не предусмотрена.

ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Оценочные и методические материалы включают в себя:
- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п\п	Контролируемые темы дисциплины	Код формируемой компетенции	Код и наименование индикатора достижения	Наименование оценочного средства
1.	Социальные, политологические и правовые аспекты, виды безопасности	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности.	Опрос
2.	Сетевые протоколы и модели взаимодействия открытых систем	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
3.	Тенденции развития безопасности операционных систем	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность	Опрос Задания для самостоятельной работы

			клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Задания для самостоятельной работы
4.	Средства и алгоритмы управления процессами, и памятью ОС	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы
5.	Безопасность клиентских приложений	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы
6.	Клиентский и серверный скрипт с позиций информационной безопасности	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и	Опрос Задания для

			серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	самостоятельной работы
7.	Каналы утечки информации. Способы несанкционированного доступа к конфиденциальной информации	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы
8.	Классы задач защиты. Стратегии защиты информации	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
9.	Понятие уязвимости информации, подходы к оценке уязвимости информации	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных	Опрос Задания для самостоятельной работы

			приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Задания для самостоятельной работы
10.	Криптографическая защита информации в Интернете	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
Результат достижения планируемых результатов изучения дисциплины				**Экзамен**

2. Описание показателей и критериев оценивания компетенций

Критерии оценивания (текущий контроль)

1. Оценка «**отлично**» выставляется студенту, если студент имеет глубокие знания учебного материала по теме практического задания, в логической последовательности излагает материал; аргументирует свою точку зрения, смог ответить на все уточняющие и дополнительные вопросы; сумел решить конкретную ситуацию, изложенную в задаче или упражнении.
2. Оценка «**хорошо**» выставляется, если студент показал знание учебного материала, смог ответить почти полностью на все заданные дополнительные и уточняющие вопросы; решил, в основном, задачу или упражнение.
3. Оценка «**удовлетворительно**» выставляется, если студент в целом освоил материал; однако, ответил не на все уточняющие и дополнительные вопросы; допустил ошибки при решении задачи; слабо ориентируется при решении конкретной ситуации.
4. Оценка «**неудовлетворительно**» выставляется студенту, если он имеет существенные пробелы в знаниях основного учебного материала по теме практического задания, который полностью не раскрыл содержание вопросов, не смог ответить на уточняющие и дополнительные вопросы; не сумел решить конкретную задачу-ситуацию.

Критерии оценивания (экзамен)

Знания, умения, навыки и компетенции студентов оцениваются следующими оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка	Критерии оценивания

Отлично	Студент не только глубоко и прочно усвоил весь программный материал, но и проявил знания, выходящие за его пределы, почерпнутые из дополнительных источников; умеет самостоятельно обобщать программный материал, не допуская ошибок, проанализировать его с точки зрения различных школ и взглядов; увязывает знания с практикой, приводит примеры, демонстрирующие глубокое понимание материала или проблемы, свободно справляется с задачами и практическими заданиями; исчерпывающе, последовательно, грамотно и логически выстраивает свой ответ.
Хорошо	Студент твердо знает программный материал, грамотно и последовательно его излагает, увязывает с практикой, не допускает существенных неточностей в ответах на вопросы, может правильно применять теоретические положения и владеет необходимыми умениями и навыками в выполнении практических заданий и решении задач, испытывает незначительные затруднения при самостоятельном обобщении программного материала.
Удовлетворительно	Студент усвоил только основной программный материал, но не знает его отдельных положений, в ответе допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала, не в полной мере владеет необходимыми умениями и навыками в выполнении практических заданий и решении задач, испытывает затруднения при самостоятельном обобщении программного материала.
Неудовлетворительно	Студент не знает значительной части основного программного материала, в ответе допускает существенные ошибки, неправильные формулировки, не владеет необходимыми умениями и навыками в выполнении практических заданий и решении задач, испытывает значительные затруднения при самостоятельном обобщении программного материала

3. Типовые контрольные задания и методические материалы, процедуры оценивания знаний, умений и навыков

Дискуссионные столы и кейс-задачи в программе не предусмотрены. Текущий контроль осуществляется по результатам выполнения заданий практикума по дисциплине «Информационная безопасность» и заданий для самостоятельной работы.

Тестовые материалы

ПАСПОРТ ТЕСТОВЫХ ЗАДАНИЙ

1. Общее количество тестовых заданий в базе – 100.
2. Ограничение времени выполнения теста (в минутах) – одна попытка, 35 минут.
3. Автоматическое перемешивание вопросов в тесте: - **да.**
4. Случайный порядок ответов в тестовом задании: - **да**.
5. Критерии оценки результатов тестирования:
   - Неудовлетворительно – 0 –55% правильных ответов.
   - Удовлетворительно -55 – 75% правильных ответов.

- Хорошо – 75 -90% правильных ответов
- Отлично – 90% и более правильных ответов

Пример тестовых заданий для текущего контроля представлен ниже:

1. Как называется свойство информации, подразумевающее возможность получения требуемой услуги за приемлемое время?
    a. Доступность.
    b. Целостность.
    c. Конфиденциальность.
2. Какой уровень модели открытых систем отвечает за управление общим доступом к сети?
    a. Прикладной уровень.
    b. Представительский уровень.
    c. Сетевой уровень.
    d. Транспортный уровень.
3. К какому уровню в модели открытых систем относится протокол TCP?
    a. Прикладной уровень.
    b. Представительский уровень.
    c. Сетевой уровень.
    d. Транспортный уровень.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Вопросы для подготовки к промежуточной аттестации по дисциплине (экзамену)

1. Основные понятия информационной безопасности – определения, руководящие документы. Угрозы информационной безопасности. Средства защиты информации.
2. Что располагается в области стандартной памяти MS-DOS.
3. Плоская модель памяти и её использование в программировании.
4. Назначение диспетчера виртуальной памяти Windows.
5. Механизм защиты процессора Intel: схемы управления памятью и защита по привилегиям
6. Права доступа к таблице страниц или к странице для программ с различными уровнями привилегий.
7. Службы управления доменом и их использование для обеспечения безопасности программ Windows.
8. Схема распределения возможного виртуального адресного пространства в системах Windows
9. Методы защиты доступа к пулам памяти.
10. Модели операционных систем –структурированная, неструктурированная и клиент – сервер.
11. Отображение виртуальной страницы памяти на физическую страницу.
12. Тест POST как средство диагностики компьютера.
13. Уровни привилегий для страниц памяти.
14. Механизм защиты процессора Intel: схемы управления памятью и защита по привилегиям.
15. Диспетчер виртуальной памяти (VMM).
16. Loadable Kernel Module атаки на операционную систему.
17. Преобразование адресов с использованием таблицы дескрипторов
18. Права доступа к таблице страниц или к странице для программ с различными уровнями привилегий.

19. Сегментация памяти в защищённом режиме
20. Логическое, линейное и физическое адресных пространства при реализации защищенного режима работы 32-разрядных процессоров
21. Механизм подключения файле config. sys драйвера himem.sys и драйвера emm386.exe
22. Механизмы защиты memory pools. Атаки на Windows NT путем воздействия на ядро операционной системы и объекты ядра.
23. Уровни привилегий супервизора (U/S = 0), пользователя (U/S = 1), как средство обеспечения безопасности страниц памяти.
24. Определение тестом POST объема установленной памяти.
25. Механизм работы Virtual Memory Manager
26. Краткая характеристика компьютерных вирусов — источники и категории атак. Стратегии взломщиков.
27. Сетевые мониторы как средство обеспечения информационной безопасности.
28. Клиентский и серверный скрипт с позиций информационной безопасности.
29. Использование JavaScript для написания клиентских скриптов. Примеры задач.
30. Создание дочерних окон средствами JavaScript в клиентских и серверных скриптах.
31. Объектно-ориентированное программирование и объекты скриптовых языков. Языки на базе классов и языки на базе прототипов.
32. Инициализация объектов в скриптовых языках.
33. Наследование свойств объектов в JavaScript.
34. Функции-конструкторы в JavaScript.
35. 16. Определение методов в JavaScript.
36. Объект Array. Создание массива, наполнение массива, Методы объекта Array.
37. Объект Document.
38. Объект Response.
39. Использование методов объекта Document и объекта Response — сравнение с позиций информационной безопасности.
40. Объект Request.
41. Передача данных методом GET.
42. Передача данных методом POST.
43. Обработка событий в ASP.
44. Поля login и password как средство обеспечения информационной безопасности.
45. Создание сайтов, в которых права доступа обеспечиваются константами, размещенными непосредственно на самих страницах.
46. Создание сайтов, в которых права доступа обеспечиваются базой данных, содержащей сведения о правах доступа.
47. Криптографическая защита информации в Интернете — симметричное и асимметричное шифрование.
48. Интернет-протоколы для защищенных соединений. Настройка SSL на стороне сервера IIS и на клиентской стороне.
49. Информационная безопасность беспроводных сетей. Технология WAP (Wireless Application Protocol). Технический стандарт RADIUS (Remote Authentication Dial-In User Service).
50. Целостность информации. Алгоритмы хэширования. Пример вычисления хэш-функции.
51. Сертификаты. Служба сертификатов Микрософт. Просмотр сертификатов на компьютере — расположение сертификатов.
52. Просмотр сертификатов на компьютере — основные поля сертификата.

53. Технология создания электронной цифровой подписи.
54. Генерация ЭЦП и проверка ЭЦП.

ГЛОССАРИЙ

Информационная безопасность – это состояние защищенности интересов субъектов информационных отношений от нежелательных действий в отношении принадлежащей им информации и информационных процессов, в которых они принимают участие.

Доступность информации – свойство системы (среды, средств и технологий ее обработки), в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и требуемая готовность соответствующих подсистем к обслуживанию поступающих запросов;

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Конфиденциальность информации – субъективно определяемое свойство информации, требующее введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней.

Уровень безопасности КС – реально достижимая степень защищенности КС и ее компонентов от прогнозируемых угроз при условии использования определенного набора сил и средств.

Угроза безопасности КС – потенциально возможное действие, событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты КС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Доступ к информации – ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации.

Правила разграничения доступа (ПРД) – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем. В подходе Гостехкомиссии НСД является ключевым понятием и трактуется как доступ к защищаемой информации с нарушением установленных прав или правил доступа, приводящий к получению субъектом возможности ознакомления с информацией и/или воздействия на нее.

Защита от НСД – предотвращение или существенное затруднение несанкционированного доступа к информации.

Канал воздействия угрозы – сочетание физической среды проникновения носителя угрозы в КС, компонента КС, на который оказывается несанкционированное воздействие, и их свойств, позволяющих угрозе реализоваться.

Способ воздействия угрозы – это последовательность действий источника (субъекта) угрозы с использованием определенных методов, средств и каналов по достижению цели реализации угрозы в отношении КС.

Видеоконференции – совокупность подключенных к Сети компьютеров, оборудованных видеокамерами, что позволяет всем участникам конференции видеть друг друга.

Вирусный маркетинг – маркетинговая техника, использующая существующие социальные сети для повышения осведомленности о бренде/товаре/услуге; стратегия, при которой товар, услуга или их реклама так влияют на человека, что он «заражается» идеей распространения определенного контента и сам становится активным ретранслятором.

Всемирная паутина (World Wide Web, WWW) – гипертекстовая информационная система, позволяющая свободно ориентироваться в Интернете, переходя от одного вопроса к другому нажатием кнопки «мыши».

Доменное имя – сетевой адрес компьютера, выраженный в буквенной форме и эквивалентный IP-адресу, который выражается в цифровой форме. Система адресации имен в Интернете имеет как свою структуру (по странам и сферам деятельности), так и свою иерархию (по уровням). Так, например, www.jf.pu.ru – принадлежит к домену третьего уровня и относится к именам, выделенным для использования в России.

Инновации – нововведения, преобразования связанные с новыми идеями, изобретениями, открытиями и т.п., а также коммерческое использование новшеств.

Интернет-мем – информация (тексты, ссылки), добровольно передаваемая пользователями друг другу, в основном в блогосфере и форумах.

Интернет-реклама – один из видов рекламы, когда носителем рекламных объявлений выступает глобальная сеть Интернет.

Интернет-СМИ – средство массовой информации, основным каналом распространения которого является Интернет.

Интерфе́йс - совокупность средств и методов взаимодействия между элементами системы.

Интерфе́йс по́льзователя – разновидность интерфейсов, в котором одна сторона представлена человеком (пользователем), другая — машиной/устройством.

Интранет – внутренняя сеть организации, доступ к ресурсам которой открыт только для членов организации.

Информационные технологии – общее название для технологий, концентрирующихся вокруг проблем обработки, хранения и управления данными.

Интернет-технологии – общее название для телекоммуникационных технологий, построенных на основе сетевой архитектуры и протоколе обмена данными TCP/IP.

Киберсквоттинг – регистрация доменных имен с целью их последующей перепродажи.

Каталог – сайт, содержащий тематически каталогизированные ссылки на интернет-сайты.

Контекстная реклама – одна из разновидностей интернет-рекламы. Специфической чертой контекстной рекламы выступает то, что пользователю «показывается» то рекламное объявление, которое соответствует контексту: поисковым запросам пользователя, соответствию условиям таргетинга, тематике рекламной площадки, журналу предыдущих посещений и т.п.

Контент – информация, размещённая на сайте. Другими словами – это содержание сайта. Контент может носить не только текстовый, но и мультимедийный характер.

Корпоративный сайт – интернет-ресурс, создаваемый с целью обеспечить полноценную двустороннюю коммуникацию базисного субъекта PR с целевыми группами общественности. Содержит информацию о сфере деятельности компании, ее структуре, производимых продуктах и т.д.

Медиапланирование – планирование размещения рекламы на рекламных носителях с целью достижения наибольшей эффективности по соотношению затраченных средств и привлечения внимания/достижения ответной реакции целевых аудиторий.

Менеджер онлайн сообщений – программа передачи мгновенных сообщений между пользователями. В отличие от чата требует установки клиентского приложения на компьютере пользователя.

Мобильный маркетинг – маркетинговая деятельность на основе технологий мобильной связи.

Навигация – система организации веб-сайта, позволяющая пользователю удобно перемещаться по сайту и легко находить необходимую информацию на нём.

Новые медиа – средства массовой коммуникации, которые обладают следующими характеристиками: цифровая форма хранения информации, сетевой способ распространения, компьютеризированная система обработки.

Оптимизация сайта – комплекс мер, направленных на получение сайтом высоких мест в результатах поиска по определенным запросам пользователей в поисковых системах.

Передача файлов по протоколу FTP и соответствующая ей система файловых архивов **FTP (FTP-service**) – 1) распределенный депозитарий, архив текстов, программ, фильмов, графических изображений, музыкальных файлов и т.д., хранящихся в виде файлов на различных компьютерах по всему миру; 2) особый протокол и клиентскую программу доступа к этим файлам.

Подкасты – аудиофайлы, предназначенные для скачивания и прослушивания в режиме оффлайн.

Поисковая машина – комплекс программ, предназначенный для поиска информации, обычно являющийся частью поисковой системы.

Поиско́вая систе́ма – веб-сайт, предоставляющий возможность поиска информации в Интернете.

Поисковый запрос – исходная информация для осуществления поиска с помощью поисковой системы.

Почтовая рассылка по списку подписчиков - метод массовой доставки полезной информации в виде электронных писем на e-mail адреса подписчиков, которые предварительно сами добровольно подписались на периодическое получение именно этой информации, обязательно подтвердив подписку на рассылку.

Прямая почтовая рассылка – инструмент прямого маркетинга (директ-маркетинга), представляющий собой метод интерактивной коммуникации через отправку писем, рекламы, листовок, образцов, проспектов и других почтовых сообщений по базе данных организаций или физических лиц, **обеспечивающий возможность обратной связи и учета ответной реакции.**

Размер аудитории сайта – количество уникальных посетителей, побывавших на сайте за определенное количество времени.

Сайт – в переводе с английского слово «сайт» означает место. Интернет-сайт является местом сосредоточения пользовательских файлов и информации, доступных через Интернет. Обычно, сайт имеет конкретный адрес или доменное имя.

Сервер интернет – компьютер, подключенный к сети, или выполняющаяся на нем программа, предоставляющие клиентам доступ к общим ресурсам и управляющие этими ресурсами.

Сервисы сети Интернет – сервисы, которые могут быть предоставлены конечному пользователю при помощи Интернета. К ним относятся: электронная почта, передача данных, поиск информации и т.п.

Скайп – программа интернет-телефонии. Позволяет не только разговаривать, но и видеть изображение собеседника, обмениваться текстовыми сообщениями и пересылать файлы.

Скрипт – программа, содержащая набор инструкций для некоторых приложений или утилит.

Тайпсквоттинг – деятельность по регистрации доменных имён, написание которых практически полностью совпадает с названиями «раскрученных» брендов или веб-сайтов. Тем самым достигается цель получения части посетителей копируемого сайта.

Таргетинг – механизм автоматического выделения целевой аудитории из всех посетителей с последующей демонстрацией необходимой рекламы. Осуществляется в соответствии с предварительно заданными параметрами и на сегодняшний день получил реализацию только в интернет-рекламе.

Технология удаленного доступа (Telnet) – технология, которая позволяет связываться с удаленным компьютером и непосредственно работать с ним.

Тэг – метка как ключевое слово, в более узком применении идентификатор, для категоризации, описания и поиска данных, задания внутренней структуры. Существует несколько основных тэгов, которые должны присутствовать в тексте любой веб-страницы. Каждая веб-страница обязана содержать тэг **<HTML>**, располагаемый в самом начале. Непосредственно за дескриптором **<HTML>** обычно следует тэг **<HEAD>**, который указывает на наличие текста, содержащего наименование страницы и дополнительные сведения о ней. В раздел HEAD обычно вложен тэг **<TITLE>**, служащий для обозначения наименования страницы. Затем следует тэг **<BODY>**, который указывает на начало собственно "тела" веб-страницы. В этом разделе размещаются весь остальной текст, графика, таблицы и другие элементы содержимого страницы, которые увидит посетитель, обратившийся к сайту.

Уникальный пользователь - пользователь, который в заданный промежуток времени может идентифицироваться как уникальный. Для его определения используется один из следующих методов (в порядке возрастания точности определения): по IP адресу; по cookies.

Фолксономия – (англ. folksonomy, от folk — народный + taxonomy таксономия, от гр. расположение по порядку + закон) — народная классификация, практика совместной категоризации информации (ссылок, фото, видео клипов и т. п.) посредством произвольно выбираемых меток, называемых тегами.

Хостинг – услуга размещения клиентских файлов на интернет-сервере. Тем самым достигается доступ к этим файлам через Интернет. Различают коммерческий и бесплатный хостинги. Тарифы на услуги хостинга сильно различаются в зависимости от набора оказываемых услуг: регистрации доменных имён, дискового пространства, установленного программного обеспечения, баз данных и т.п.

Целевые посетители сайта — группа интернет-пользователей, на которую сфокусировано содержание сайта; круг посетителей, заинтересованных в информации, товарах или услугах, представленных на сайте.

Чат – в переводе с английского слово «чат» означает «разговор». Чат – это организация разговора при помощи веб-интерфейса. Обычно, разговор ведётся при помощи текстовых сообщений на специальном разделе интернет-сайта. В отличие от веб-мессенджеров чат не требует установки приложений на компьютер пользователя.

Электронная коммерция – любые формы торговых сделок, при которых взаимодействие сторон осуществляется с применением возможностей информационных и телекоммуникационных технологий

Электронная почта – интернет-сервис, позволяющий отправлять, получать и хранить электронные сообщения. Также позволяет пересылать файлы. Основной инструмент официального или делового общения в Интернете.

Электронный бизнес – процессы внедрения и использования новых информационных технологий, вычислительной техники, телекоммуникационных сетей (включая Интернет) для достижения бизнес-задач.

Электронный маркетинг – теория и методология организации маркетинговой деятельности при помощи современных информационных технологий.

Юзабилити – удобство использования сайта для его посетителей, логичность и простота в расположении элементов управления.

Alt tag - тэг альтернативного текста, который показывает браузер, когда пользователь не хочет или не может видеть изображение на веб-странице. Использование в коде страницы alt-тэгов, содержащих ключевые слова (keywords), может повысить рейтинг страницы в листе ответов поисковой системы.

ARG (Alternative Reality Games) – интерактивное повествование с игровыми элементами, использующее в качестве платформы реальный мир.

BTL (от англ. below-the-line – под чертой) – комплекс маркетинговых коммуникаций, отличающихся от прямой рекламы ATL (от англ. above-the-Line) уровнем воздействия на потребителей и выбором средств воздействия на целевую аудиторию. Включает в себя стимулирование сбыта, мерчандайзинг, POS-материалы (аббр. от англ. point of sale — место продажи), директ мейл (от англ. direct mail — прямые почтовые рассылки), выставки и многое другое.

CTR (click through rate) – «кликабельность» – соотношение количества показов рекламного объявления к кликам пользователей.

CMS (Content Management System) – программное обеспечение, делающее публикацию сообщений на сайте легкой, быстрой и не требующей от пользователя специальных навыков и знаний.

Cookies – небольшие файлы, которые сохраняются на компьютере пользователя и содержат подробную информацию о его поисковой активности.

CPA (cost per action) – метрика, которая определяет стоимость одного совершенного на сайте действия (например, заполнения формы обратной связи или отсылку письма).

DNS (Domain Name Service) – система доменных имен, обеспечивающая возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов.

HTML (**HyperText Markup Language**) – язык, используемый для указания формата и содержания документа в WWW (например, в веб-страницах). Браузер распознает директивы языка HTML и автоматически показывает результаты на экране.

HTTP (Hypertext Transfer Protocol) – протокол, используемый для доступа к документам WWW.

IP-адрес – уникальный числовой адрес, присваиваемый каждому компьютеру, подключенному к сети Интернет. Состоит из четырех групп чисел (до 255), разделенных точками.

IP/TCP протоколы – фундаментальный набор сетевых протоколов, обеспечивающих работу Интернета.

PDA (Personal Digital Assistant) **–** карманные персональные компьютеры.

RSS – формат распространения новостей, позволяющий автоматически при помощи специальных программ-агрегаторов или браузеров получать обновления с сайтов, блогов, лент новостей и т.п.

SEO (Search Engine Optimization) – поисковая оптимизация сайта с целью вывода ссылки на него в число первых, отображаемых в ответ на запрос пользователя.

SEO копирайтинг – определенная техника создания и редактирования текстов для сайтов таким образом, чтобы, во-первых, пользователь мог легко прочитать и понять текст,

и, во-вторых, чтобы при этом текст содержал необходимые для продвижения в поисковых системах ключевые слова в нужных местах и в необходимых пропорциях.

SMM (Social Media Marketing) – маркетинг в социальных медиа.

SMO (Social media optimization*)* – комплекс мер, направленных на привлечение на сайт посетителей из социальных сетей. SMO – прежде всего меры по техническому изменению сайта для повышения совместимости с социальными сетями, но часто под данной аббревиатурой подразумевают и комплекс мер по PR в социальных сетях.

URL (Uniform Resource Locator) – уникальный адрес, которым обладает каждая веб-страница в сети. Если пользователю известен URL страницы, то он может ее отобразить у себя в браузере, набрав ее адрес в строке браузера.

Wi-Fi (англ. – **Wi**reless **Fi**delity) – это стандарт беспроводного доступа к Интернету.

WWW (World Wide Web) – см. Всемирная паутина

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЯ ПО ДИСЦИПЛИНЕ

Основной целью изучения дисциплины «**Информационная безопасность**» является исследование различных видов информационных угроз (включая компьютерные вирусы) и методов противодействия им; основных принципов и стандартов; различных профилей информационной безопасности; видов политики обеспечения информационной безопасности.

Дисциплина изучает различные аспекты информационной безопасности, алгоритмы управления процессами и ресурсами операционной системы, подходы к защите информации при использовании клиентских и серверных скриптов.

Форма промежуточной аттестации знаний – **экзамен**.

Методические принципы и приемы построения учебной дисциплины «информационная безопасность». Ключевыми методическими способами подачи учебного материала по дисциплине «информационная безопасность» являются лекции и семинарские занятия.

Лекционное занятие **–** это систематическое, последовательное, устное изложение лектором учебного материала. Занятие «лекция» носит, прежде всего, обзорный характер, охватывая весь круг выносимых на изучение учебных вопросов. При проведении такого типа занятий очень важно живое слово лектора, его педагогическое мастерство как педагога, который дает студентам информационную базу. Лекции являются важной формой передачи преподавателем студентам общетеоретических знаний.

Лекции, как правило, читаются не по всем, а по наиболее сложным темам курса, не дублируют учебники, а содержат новейшие научные данные и примеры, которых может не быть в учебных пособиях. Для лучшего усвоения материала на лекционных занятиях целесообразно предварительно перед лекцией ознакомиться с положениями лекционной темы в конспекте лекций, содержащемся в данном учебно-методическом пособии либо в рекомендуемых учебниках.

Подгрупповые занятия **–** другая важная форма учебного процесса. Они способствуют закреплению и углублению знаний, полученных студентами на лекциях и в результате самостоятельной работы над научной и учебной литературой и нормативными источниками. Они призваны развивать самостоятельность мышления, умение делать выводы, связывать теоретические положения с практикой, формировать профессиональное правовое сознание. На занятиях вырабатываются необходимые каждому бакалавру навыки и умения публично выступать, логика доказывания, культура профессиональной речи. Кроме того, семинары – это средство контроля преподавателей за самостоятельной работой студентов, они непосредственно влияют на уровень подготовки к итоговым формам отчетности – зачетам и экзаменам. В выступлении на семинарском занятии должны содержаться следующие элементы:

- четкое формулирование соответствующего теоретического положения в виде развернутого определения;
- приведение и раскрытие основных черт, признаков, значения и роли изучаемого явления или доказательства определенного теоретического положения;
- подкрепление теоретических положений конкретными фактами.

Для качественного и эффективного изучения актуальных проблем теории необходимо овладение навыками работы с книгой, воспитание в себе стремления и привычки получать новые знания из научной и иной специальной литературы. Без этих качеств не может быть настоящего специалиста ни в одной области деятельности.

Читать и изучать, следует, прежде всего, то, что рекомендуется к каждой теме программой, планом семинарских занятий, перечнем рекомендуемой литературы.

Когда студент приступает к самостоятельной работе, то он должен проявить инициативу в поиске специальных источников. Надо иметь в виду, что в каждом последнем номере издаваемых журналов публикуется библиография всех статей, напечатанных за год, это облегчает поиск нужных научных публикаций.

Работа с научной литературой, в конечном счете, должна привести к выработке у бакалавра умения самостоятельно размышлять о предмете и объекте изучения, которое должно проявляться:

- в ясном и отчетливом понимании основных понятий и суждений, содержащихся в публикации, разработке доказательств, подтверждающих истинность тех или иных положений;
- в понимании студентами обоснованности и целесообразности, приводимых в книге и статье примеров, поясняющих доказательства и выводы автора. При этом будет уместно, если бакалавр самостоятельно приведет дополнительные примеры к этим выводам;
- в отделении основных положений от дополнительных, второстепенных сведений;
- в способности студента критически разобраться в содержании публикации, определить свое отношение к ней в целом, дать ей общую оценку, характеристику.

Другим важнейшим методическим приемом в учебном процессе является самостоятельная работа студента.

Самостоятельная работа в высшем учебном заведении, является важной организационной формой индивидуального изучения студентами программного материала.

В современных условиях дидактическое значение самостоятельной подготовки неизмеримо возрастает, а ее цели состоят в том, чтобы:

- повысить ответственность самих обучаемых за свою профессиональную подготовку, сформировать в себе личностные и профессионально-деловые качества;
- научить студентов самостоятельно приобретать знания, формировать навыки и умения, необходимы для юридической деятельности;
- развивать в себе самостоятельность в организации, планировании и выполнении заданий, определяемых учебным планом и указаниями преподавателя.

Достигнуть этих целей в ходе самостоятельной работы при изучении дисциплины возможно только при хорошей личной организации своего учебного труда, умении использовать все резервы имеющегося времени и подчинить их профессиональной подготовке.

Самостоятельная работа как метод обучения включает:

- изучение и конспектирование обязательной литературы в соответствии с программой дисциплины;
- ознакомление с литературой, рекомендованной в качестве дополнительной;
- изучение и осмысление специальной юридической терминологии и понятий;
- изучение и отработка нормативных актов, комментариев к ним, проведение сравнительного анализа с предыдущим;
- сбор материала и написание контрольных, конкурсных и дипломных работ;
- изучение указанной литературы для подготовки к зачету.
- Основными компонентами содержания данного вида работы являются:
- творческое изучение учебных пособий и научной литературы;
- умелое конспектирование;

- участие в различных формах учебного процесса, научных конференциях, в работе кружков и т. д.;
- получение консультаций у преподавателя по отдельным проблемам курса;
- получение информации и опыта о работе профессионалов в процессе производственно-учебной практики;
- знакомство со специальной литературой при формировании своей личной библиотеки и др.

Данный комплекс рекомендаций позволяет студентам овладеть многими важными приемами самостоятельной работы и успешно использовать их при подготовке контрольных по дисциплине.

Важнейшей формой учебной отчетности студента является **контрольная работа.** Выполнение контрольной работы является промежуточной формой отчетности по изучаемой дисциплине и преследует цель лишь оценить способность студента к самостоятельному поиску источников, формированию содержания и его письменного изложения по указанной проблеме. Это важная составляющая изучения дисциплины, а также эффективная форма контроля знаний. При заочном обучении она выступает как обязательная, основная форма самостоятельной работы. В контрольной работе (в соответствии с учебным планом) студент обязан самостоятельно глубоко разобраться в изучаемых проблемах, усвоить суть темы, уяснить ее содержание и только затем письменно представить свою отчетную работу.

Выполнение контрольной работы является одним из условий допуска студента к сдаче зачета. Работа должна соответствовать установленным требованиям, то есть в ней должны быть раскрыты все проблемы, определенные темой. Для этого студент обязан самостоятельно проанализировать первоисточники и дать исчерпывающие ответы на вопросы темы. Контрольная работа — серьезное учебное задание, и чтобы написать ее как следует, необходимо использовать те первоисточники и учебные пособия, которые позволяют полнее разобраться в проблеме. Бакалавр должен регулярно работать в университетской и городской библиотеке, вдумчиво конспектировать лекции преподавателей.

При написании контрольной работы следует обращать особое внимание на грамотное использование юридической терминологии. При употреблении впервые тех или иных терминов и понятий следует давать их определения либо в самом тексте, либо в сносках.

Приступая к контрольной работе, требуется сначала ознакомиться с имеющейся литературой по теме, изучить первоисточники и составить план. Здесь, в отличие от курсовой работы, план предполагает рассмотрение одной, причем довольно широкой, проблемы, и он может состоять из двух-трех вопросов. Минимальное количество первоисточников, привлекаемых для написания контрольной работы — пять наименований.

Контрольные работы могут выступать как дополнительные (вспомогательные) учебные формы отчетности студента, которые осуществляются в ходе семинарских (практических) занятий (в конце) и проводятся максимум в течение 10-15 минут. Преподаватель может заранее объявить о предстоящей работе и предложить примерный перечень тем, то есть сориентировать студентов на работу по более широкому кругу вопросов. Таким образом, бакалаврам дается возможность лишний раз обратиться к учебному материалу и более качественно подготовиться к выполнению контрольной работы.

Как правило, контрольные работы по дисциплине сугубо индивидуальны, то есть их тематика персонифицирована. Однако в отдельных случаях темы контрольных работ могут

быть адресованы и сразу нескольким бакалаврам, и группе в целом. Таким приемом преподаватель выявляет степень усвоения какой-то важной учебной проблемы и определяет необходимость проведения дополнительных занятий по какой-либо теме.

В качестве контрольной работы широко применяется самостоятельное изучение монографического исследования по конкретной, крайне важной проблеме, требующей глубокого рассмотрения. Этот вид работы предполагает не простое знакомство с определенным монографическим исследованием, а детальное его изучение. Для этого студенту важно знать некоторые правила работы с первоисточником, которым для него будет являться монография. Следует выяснить фамилию автора, его имя и отчество, ученую степень и звание, а также что побудило его взяться за изучение данной проблемы;

обратить внимание на основные вопросы монографии и их разрешение автором, уметь раскрывать их в ходе собеседования с преподавателем.

Студенту следует письменно (предельно кратко) очертить те вопросы (полностью или частично), которые поставлены автором в монографическом исследовании; при изложении их следует указывать страницы источника.

Особую инновационность в методическом плане при преподавании дисциплины «Документоведение и документальное обеспечение управления» представляют ролевые и деловые игры как форма коллективной деятельности педагога и студентов при проведении семинарских занятий.

Игра позволяет влиять на правовые установки студентов. Учебно-правовые ситуации относятся к тем методическим средствам, которые позволяют осуществлять взаимосвязь понятийно-категориального уровня правосознания с поведенческим. В результате достигается не только интеллектуальный, но и эмоциональный уровень усвоения правовых понятий и идей.

Учебно-тренировочные ситуации являются специфическим методическим приемом, одним из основных видов проблемно-развивающего обучения, благодаря которому усиливается практический интерес бакалавров к теоретико-правовым вопросам.

Эффективность применения учебных ситуаций зависит от соблюдения следующих условий: знание студентами теоретического материала и наличие достаточного личного опыта и жизненного опыта вообще.

Важными в методическом плане на семинарских занятиях являются проводимые **тестовые опросы** и решение задач, которые содействуют превращению знаний в глубокие убеждения, дают простор для развития творческо-эмоциональной сферы, позволяют сделать выводы об эффективности занятий с учащимися, что в итоге повышает интерес к овладению знаниями.

Только сочетая дидактически и органически все методические способы и приемы в их диалектическом единстве и взаимосвязи мы можем добиться должного уяснения учебного материала со стороны студентов.

Методические рекомендации для преподавателей

Тема занятия	Виды учебных занятий	Способы учебной деятельности	Методы обучения, формы педагогического общения	Средства обучения	Формы контроля
1	*2*	*3*	*4*	*5*	*6*
Социальные, политологические и правовые аспекты, виды безопасности	Подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Сетевые протоколы и модели взаимодействия открытых систем	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Тенденции развития безопасности операционных систем	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятe

					льного выполнения, экзамен.
Средства и алгоритмы управления процессами, и памятью ОС	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Безопасность клиентских приложений	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Клиентский и серверный скрипт с позиций информационной безопасности	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Каналы утечки	Лекция,	Коллективный,	Лекция, рассказ	Ноутбук,	Аттестация

информации. Способы несанкционированного доступа к конфиденциальной информации	подгрупповое занятие	Индивидуально-групповой	объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Классы задач защиты. Стратегии защиты информации	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Понятие уязвимости информации, подходы к оценке уязвимости информации	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог частично-поисковый, дискуссия.	Ноутбук, проектор, компьютеры с установленным программным обеспечением, презентация, электронный курс по дисциплине	Аттестация в компьютерном классе (по Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.
Криптографическая защита информации в Интернете	Лекция, подгрупповое занятие	Коллективный, Индивидуально-групповой	Лекция, рассказ объяснительно-иллюстративный, монолог, внешний диалог	Ноутбук, проектор, компьютеры с установленным программным	Аттестация в компьютерном классе (по

			частично-поисковый, дискуссия.	обеспечением, презентация, электронный курс по дисциплине	Университетскому графику), проверка заданий для самостоятельного выполнения, экзамен.

Приложение

Тематический план изучения дисциплины «Информационная безопасность»

Год набора с 2020 форма обучения заочная

Наименование разделов и тем	**Всего**	**Трудоемкость по дисциплине**					**Формируемые компетенции**
		Контактная работа	в т.ч.			СР	
			Лекции	Подгр/ лаб	Пр/Сем		
Социальные, политологические и правовые аспекты, виды безопасности	19	4	2	2	0	15	ОПК-3
Сетевые протоколы и модели взаимодействия открытых систем	19	4	2	2	0	15	ОПК-3
Тенденции развития безопасности операционных систем	19	4	2	2	0	15	ОПК-3
Средства и алгоритмы управления процессами, и памятью ОС	23	8	2	6	0	15	ОПК-3
Безопасность клиентских приложений	21	6	2	4	0	15	ОПК-3
Клиентский и серверный скрипт с позиций информационной безопасности	21	6	2	4	0	15	ОПК-3
Каналы утечки информации. Способы несанкционированного доступа к конфиденциальной информации	21	6	2	4	0	15	ОПК-3
Классы задач защиты. Стратегии защиты информации	16	6	2	4	0	10	ОПК-3
Понятие уязвимости информации, подходы к оценке уязвимости информации	16	6	2	4	0	10	ОПК-3
Криптографическая защита информации в Интернете	14	4	0	4	0	10	ОПК-3
Контроль	**27**						
Итого по дисциплине	**216**	**54**	**18**	**36**	**0**	**135**	
Зачетных единиц	**6**						

Тематический план изучения дисциплины «Информационная безопасность»

Год набора с 2020 форма обучения заочная

Наименование разделов и тем	**Всего**	**Трудоемкость по дисциплине**					**Формируемые компетенции**
		Контактная работа	в т.ч.			СР	
			Лекции	Подгр/ лаб	Пр/Сем		
Социальные, политологические и правовые аспекты, виды безопасности	13	2	2	0	0	11	ОПК-3
Сетевые протоколы и модели взаимодействия открытых систем	22	2	2	0	0	20	ОПК-3
Тенденции развития безопасности операционных систем	22	2	0	2	0	20	ОПК-3
Средства и алгоритмы управления процессами, и памятью ОС	22	2	0	2	0	20	ОПК-3
Безопасность клиентских приложений	22	2	0	2	0	20	ОПК-3
Клиентский и серверный скрипт с позиций информационной безопасности	22	2	0	2	0	20	ОПК-3
Каналы утечки информации. Способы несанкционированного доступа к конфиденциальной информации	20	0	0	0	0	20	ОПК-3
Классы задач защиты. Стратегии защиты информации	22	2	0	2	0	20	ОПК-3
Понятие уязвимости информации, подходы к оценке уязвимости информации	20	0	0	0	0	20	ОПК-3
Криптографическая защита информации в Интернете	22	2		2	0	20	ОПК-3
Контроль	**9**	**9**					
Итого по дисциплине	**216**	**25**	**4**	**12**		**191**	
Зачетных единиц	**6**						
Контрольная работа	**+**						