

Министерство культуры Российской Федерации  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«КРАСНОДАРСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ  
КУЛЬТУРЫ»**

Информационно-библиотечный факультет  
Кафедра документоведения и информационной культуры

УТВЕРЖДАЮ  
Зав. кафедрой  
документоведения  
и информационной культуры  
Н.Б.Зиновьева  
26.08. 2015 г.

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ  
УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.Б.20 Информационная безопасность и защита информации**  
Направление подготовки **46.03.02 – Документоведение и архивоведение**  
Профиль подготовки **Делопроизводство в органах исполнительной власти и местного самоуправления**  
Квалификация (степень) выпускника **-бакалавр**  
Форма обучения - очная, заочная

Составитель:  
Мельникова А.В., к.п.н., ст. преподаватель

 (подпись) \_\_\_\_\_ ( Ф.И.О.)

Краснодар 2015

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Целями** освоения дисциплины (модуля) «Информационная безопасность и защита информации» являются формирование у студентов системы концептуальных представлений и практических навыков по защите информации, анализу, оценке, отбору и использованию средств, обеспечивающих информационную безопасность.

### **Задачи:**

- владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения;
- развитие способности критически воспринимать и оценивать источники информации,
- умение четко и логично формулировать, излагать и аргументировано отстаивать собственное видение проблем и способов их разрешения.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина читается в цикле специальных дисциплин.

Изучение дисциплины базируется на знании студентами следующих дисциплин учебного плана: «Документоведение», «Информационная культура личности», «Информационное право», «Информационные технологии».

## 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

ОК-1 владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения;

ОК-6 способностью использовать нормативные правовые акты в своей деятельности;

ОК-9 способностью понимать сущность и значение информации в развитии современного общества, осознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;

ОК-12 владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;

ПК-3 владеть знаниями в области права (административное, гражданское, трудовое, специальное).

ПК-32 владеть навыками работы с документами, содержащими информацию ограниченного доступа.

ПК-40 владеть методами защиты информации.

В результате обучения студенты должны **знать:**

содержание базовых понятий "защита информации", "информационная безопасность", "информация с ограниченным доступом", "угрозы информационной безопасности", "дестабилизирующие факторы", "утечка информации", "каналы утечки", "криптографическая защита информации", "защита информации от

несанкционированного доступа";

виды защищаемой информации (государственная тайна, конфиденциальная информация, информация, затрагивающая неприкосновенность частной жизни, коммерческая, профессиональная, служебная тайна);

основные нормативные документы, регулирующие деятельность по защите информации и определяющие функционирование государственной системы защиты информации;

источники и виды угроз информационной безопасности, методы противодействия угрозам;

цели и методы деятельности органов добывания информации;

особенности каналов утечки информации и способы предотвращения утечки;

алгоритм действия криптографических систем защиты информации, обеспечивающих конфиденциальность, проверку авторства и целостности электронных документов;

принципы построения систем защиты информации от несанкционированного доступа и требования, предъявляемые к этим системам;

основные виды компьютерных вирусов и других программ с потенциально опасными последствиями, способы борьбы с вирусами и программными закладками;

особенности работы в общедоступных компьютерных сетях (в т.ч. в Интернет) с точки зрения информационной безопасности;

цель, задачи и порядок деятельности службы информационной безопасности предприятия;

**уметь:**

структурировать защищаемую информацию и определять правовую основу ее защиты;

устанавливать и ранжировать угрозы информационной безопасности;

оценивать целесообразность и эффективность применения основных методов защиты информации;

разрабатывать предложения по предотвращению утечки информации по оптическому, акустическому, радиоэлектронному и материально-вещественному каналам;

применять технологии шифрования и электронной цифровой подписи электронных документов;

формулировать задачи по обеспечению защиты информации от несанкционированного доступа, в т.ч. в компьютерных сетях (включая Интернет);

классифицировать компьютерные вирусы и выработать предложения по предупреждению заражения компьютеров, обнаружению и удалению вирусов;

работа в составе службы информационной безопасности предприятия (в т.ч. определять перечень сведений, составляющих коммерческую тайну);

**иметь представление:**

о современных тенденциях развития основных средств защиты информации;

о порядке лицензирования деятельности, сертификации продуктов и услуг в сфере защиты информации;

об организационном и документационном обеспечении информационной безопасности и защиты информации.

#### **4. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ**

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 часа). Дисциплина реализуется в 5 семестре. Форма промежуточной аттестации – зачет в 5 семестре.