**ПРОГРАММа УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Информационная безопасность**

(УГЛУБЛЕННАЯ ПОДГОТОВКА)

2014 г.

Программа учебной дисциплины Информационная безопасность разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) **230115 Программирование в компьютерных системах** по программе углубленной подготовки

Организация-разработчик: Областное государственное бюджетное профессиональное образовательное учреждение Смоленская академия профессионального образования

Разработчик:

Ромашкова И.А., преподаватель ОБГПОУ СмолАПО

Утверждена Научно-методическим советом ОБГПОУ СмолАПО

Протокол № 1 от 05.09.2014 г.

Рассмотрена на заседании кафедры Информационных технологий

Протокол № 1 от 02.09.2014 г.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
|  | стр. |
| ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ | 4 |
| Результаты освоения учебной дисциплины | 5 |
| СТРУКТУРА и содержание УЧЕБНОЙ ДИСЦИПЛИНЫ | 6 |
| условия реализации программы учебной дисциплины | 13 |
| Контроль и оценка результатов Освоения учебной дисциплины | 14 |

**1. паспорт ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Информационная безопасность**

**1.1. Область применения программы**

Программа учебной дисциплины *Информационная безопасность* является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО *230115 Программирование в компьютерных системах углубленной подготовки.*

**1.2. Место дисциплины в структуре основной профессиональной образовательной программы:** дисциплина *Информационная безопасность* является общепрофессиональной дисциплиной профессионального цикла дисциплин по специальности вариативной части основной профессиональной образовательной программы.

Обеспечивающие дисциплины: теория вероятностей и математическая статистика, операционные системы, архитектура компьютерных систем, технические средства информатизации, информационные технологии, основы программирования, математическое моделирование.

**1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:**

В результате освоения дисциплины обучающийся должен

*уметь:*

* классифицировать основные угрозы безопасности информации;
* применять организационные, правовые, программно-технические, криптографические методы и средства защиты информации;
* применять антивирусные средства защиты информации.

В результате освоения дисциплины обучающийся должен

*знать:*

* сущность и понятия информационной безопасности;
* основные угрозы, методы и средства обеспечения информационной безопасности;
* принципы защиты информации от несанкционированного доступа;
* правила применения, эксплуатации и обслуживания технических средств защиты информации

**1.4. Рекомендуемое количество часов на освоение программы дисциплины:**

максимальной учебной нагрузки обучающегося 156 часа /4 зач.ед, в том числе:

* обязательной аудиторной учебной нагрузки обучающегося 104 часов;
* самостоятельной работы обучающегося 52 часа.

**2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

Результатом освоения учебной дисциплины является овладение общими (ОК) и профессиональными (ПК) компетенциями:

|  |  |
| --- | --- |
| **Код** | **Наименование результатов обучения** |
| ОК 1. | Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес |
| ОК 2. | Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. |
| ОК 3. | Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях. |
| ОК 4. | Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития. |
| ОК 5. | Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности. |
| ОК 6. | Работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7. | Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий. |
| ОК 8. | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9. | Быть готовым к смене технологий в профессиональной деятельности. |
| ПК 3.3. | Выполнять отладку программного продукта с использованием специализированных программных средств |
| ПК 5.1. | Производить инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем |

**3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**3.1. Объем учебной дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | ***Объем часов***  ***/ зачетных единиц*** |
| **Максимальная учебная нагрузка (всего)** | 156/4 |
| **Обязательная аудиторная учебная нагрузка (всего)** | 104 |
| в том числе: |  |
| семинары | 72 |
| лабораторные занятия | - |
| практические занятия | 30 |
| контрольные работы | 2 |
| **Самостоятельная работа обучающегося (всего)** | 52 |
| в том числе: |  |
| *разработка опорных конспектов*  *выполнение таблиц, схем шифрования, презентаций для систематизации учебного материала*  *выполнение упражнений, решение ситуаций и задач*  *написание реферата*  *изучение и анализ законодательных актов, стандартов, руководящих документов* | 8  12  14  6  12 |
| *Итоговая аттестация в форме экзамена* | |

**3.2. Тематический план и содержание учебной дисциплины Информационная безопасность**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование разделов и тем** | | | **Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся** | **Объем часов** | **Уровень освоения** |
| **1** | | | **2** | **3** | **4** |
| **Раздел 1. Информационная безопасность. Основные положения, понятия, определения** | | | | **18** |  |
| **Тема 1.1.**  **Сущность и понятие информационной безопасности** | | | Содержание учебного материала | **8** | *2,3* |
| Национальные интересы в информационной сфере. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. Информационная безопасность в системе национальной безопасности Российской Федерации. Современная концепция информационной безопасности. Доктрина информационной безопасности. Информационные ресурсы. Информационные войны. |
| Практические занятия  *Анализ Доктрины информационной безопасности* | 2 |  |
| Семинарские занятия  Тема: *Основы государственной информационной политики и информационной безопасности Российской Федерации*   1. Сущность и понятие информационной безопасности, характеристика ее составляющих. 2. Национальные интересы в информационной сфере. 3. Информационная безопасность в системе национальной безопасности Российской Федерации 4. Место информационной безопасности в системе национальной безопасности.   Тема:*Общие подходы к определению информационной безопасности*   1. Современная концепция информационной безопасности. 2. Термины и определения информационной безопасности. 3. Доктрина информационной безопасности.   Тема: *Информация – наиболее ценный ресурс современного общества*   1. Информационные ресурсы. 2. Информационные войны. 3. Информационное оружие и его классификация. | 6 |
| *Самостоятельная работа обучающихся*  Составление глоссария «Введение в основы информационной безопасности»  Выполнение таблицы «Интересы Российской Федерации в информационной сфере» | 4 |
| **Тема 1.2.**  **Правовые основы защиты информации** | | | Содержание учебного материала | **10** | 2,3 |
| Основные законодательные акты Российской Федерации в области защиты информации. Источники права на доступ к информации. Уровни и виды доступа. Управление доступом. Ответственность за нарушение законодательства в информационной сфере. |
| Практические занятия  *Изучение Российского законодательства по защите информационных технологий* | 2 |  |
| Семинарские занятия  Тема: *Правовые основы защиты информации*   1. Опыт законодательного регулирования информатизации в России и за рубежом. 2. Концепция правового обеспечения информационной безопасно­сти Российской Федерации. 3. Стандарты и нормативно-методические доку­менты в области обеспечения ИБ. Государст­венная система ОИБ. 4. Международ­ные правовые акты по защите информации.   Тема: *Законодательное регулирование информатизации в России*   1. Уровни доступа к информации с точки зрения законодательства. 2. Информация ограниченного распространения. 3. Виды ответственности за нарушение законодательства в информационной сфере. | 8 |
|  | | | *Самостоятельная работа обучающихся*  Составление перечня законодательных актов в области защиты информации  Подготовка опорного конспекта «Ответственность за нарушение законодательства в информационной сфере»  Сравнительный анализ международных и государственных стандартов информационной безопасности | 5 |
| **Раздел 2. Сущность и понятие защиты информации** | | | | **22** |  |
| **Тема 2.1 Основы защиты информации** | | | Содержание учебного материала | **4** | 2,3 |
| Цели и задачи защиты информации. Концептуальные основы защиты информации. Источники и носители защищаемой информации. |
| Семинарское занятие  Тема: *Источники и носители защищаемой информации*   1. Понятие «информационный ресурс», классы информационных ресурсов. 2. Источники и носители защищаемой информации, их классификация. 3. Источники сигналов. | 4 |  |
| *Самостоятельная работа обучающихся*  Электронное конспектирование с комментариями «Информация, сообщения, информационные процессы как объекты информационной безопасности»  Создание классификационной схемы понятий в области « Защита информации» | 2 |
| **Тема 2.2. Конфиденциальная информация** | | | Содержание учебного материала | **8** | 2,3 |
| Понятие о конфиденциальной информации. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Защита конфиденциальной информации |
| Семинарские занятия  Тема: *Конфиденциальная информация.*   1. Понятие о конфиденциальной информации. 2. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. 3. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.   Тема: *Отнесение информации по видам тайн*   * 1. Защита конфиденциальной информации.   2. Отнесение циркулирующей в организации информации по видам тайн. | 8 |  |
| *Самостоятельная работа обучающихся*  Создание таблицы для систематизации знаний «Классификация информации с точки зрения ее владельца»  Выполнение упражнений на отнесение циркулирующей в организации информации по видам тайн | 4 |
| **Тема 2.3. Угрозы информационной безопасности** | | Содержание учебного материала | | **10** | 2,3 |
| Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Методы оценки уязвимости информации. Виды утечки информации. Источники рисков и формы атак на информацию. | |
| Семинарские занятия  Тема: *Понятие угрозы безопасности информации*   1. Понятие угрозы безопасности информации 2. Классификация угроз безопасности информации. 3. Виды утечки информации.   Тема: *Оценки уязвимости информации*   1. Методы оценки уязвимости информации 2. Выявление и определение степени вероятности угроз объекту информатизации.   Тема*: Принципы воздействия на СОИ*   1. Характер воздействия на СОИ. 2. Способы активного воздействия на объект атаки. 3. Формы атак на информацию. 4. Каналы несанкционированного получения информации в СОИ. | | 9 |  |
| Контрольная работа по теме «Сущность и понятие защиты информации» | | 1 |
| *Самостоятельная работа обучающихся*  Составление классификационной схемы «Угрозы информационной безопасности»  Выполнение индивидуального проектного задания «Классификация угроз безопасности информации на типовом объекте информатизации» | | 5 |
| **Раздел 3. Методы и средства борьбы с угрозами информационной безопасности систем обработки информации** | | | | **62** |  |
| **Тема 3.1. Обеспечение безопасности систем обработки информации** | | Содержание учебного материала | | **26** | *2,3* |
| Основные направления борьбы с угрозами безопасности СОИ. Разграничение доступом к ресурсам систем обработки информации. Идентификация и аутентификации информационной безопасности. Парольные системы для защиты от несанкционированного доступа к информации. Криптографические методы защиты информации. | |
| Практические занятия  *Изучение принципов идентификации и механизмов подтверждения подлинности пользователя.*  *Установка и настройка оборудования - средства аутентификации «Рутокен»*  *Изучение правил формирования электронной цифровой подписи*  *Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации*  *Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем*  *Шифрование информации различными методами* | | 12 |  |
| Семинарские занятия  Тема: *Основные направления борьбы с угрозами безопасности СОИ*   1. Требования по защите средств вычислительной техники и автоматизированных систем от НСД. 2. Классы защищенности средств вычислительной техники от НСД и показатели защищенности. 3. Классы защищенности автоматизированных систем от НСД и показатели защищенности. 4. Критерии оценки безопасности информационных технологий   Тема: *Обеспечение безопасности систем обработки информации*   1. Идентификация и аутентификация. 2. Разграничение доступа к элементам защищаемой информации. 3. Парольные системы для защиты от несанкционированного доступа к информации. Выбор паролей, хранение паролей.   Тема*: Криптографические методы защиты*   1. Требования к СКЗИ 2. Классификация методов криптографического закрытия. 3. Криптографические системы. 4. Применение криптографических методов и средств. Электронная подпись.   Тема: *Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем*   1. Стандартные алгоритмы шифрования. Основные понятия и определения. 2. Шифры перестановки. Шифрующие таблицы. 3. Безопасность и быстродействие криптосистемы. 4. Отечественный стандарт шифрования данных. | | 14 |
| *Самостоятельная работа обучающихся*  Составление опорного конспекта «Показатели защищенности средств вычислительной техники и АС от НСД»  Выполнение упражнений на шифрование и дешифрование информационных сообщений различными методами.  Подготовка презентации на тему: «Методы криптографического закрытия» | | 14 |
| **Тема 3.2** **Программно-технические угрозы информационной безопасности СОИ методы и средства борьбы с ними** | | Содержание учебного материала | | **24** | *2,3* |
| Программно-технические угрозы информационной безопасности ПК. Средства вторжения в частную жизнь. Понятие, пути распространения, проявления действия вируса. Классификация вирусов. Структура современных вирусов. Модели поведения вирусов. Программы-шпионы. Классификация антивирусных программ. Аппаратно-программные комплексы криптографической защиты. Средства защиты информации от утечки по каналам ПЭМИН. | |
| Практические занятия  *Изучение средств программной защиты ПК*  *Установка и настройка оборудования - аппаратного комплекса защиты конфиденциальной информации «Aladdin. SecretDisk», биометрической флэш – памяти nTegrity Pro Vista*  *Установка и настройка оборудования - мышь со считывателем отпечатка пальца – EyeD Opti Mouse*  *Установка и настройка оборудования - комплекс СЗИ НСД «Аккорд - АМДЗ», АПМДЗ «КРИПТОН - ЗАМОК»*  *Установка и обновление баз данных антивирусных программ, настройка антивирусной защиты* | | 10 |  |
| *Тема: Компьютерные вирусы*   1. Программно-технические угрозы информационной безопасности ПК. 2. Средства вторжения в частную жизнь. 3. Программы-шпионы.   Тема: *Пути распространения, проявления действия вируса*   1. История развития компьютерных вирусов 2. Методы распространения компьютерных вирусов 3. Деструктивные возможности компьютерных вирусов.   Тема: *Классификация антивирусных программ*   1. Программы-детекторы 2. Программы-доктора 3. Программы-ревизоры 4. Программы-фильтры   Тема: *Аппаратно-программная защита информации*   1. Типы аппаратно-программных комплексов криптографической защиты 2. Состав СКЗИ 3. Особенности устройств. 4. Динамические библиотеки СКЗИ   Тема: *Средства защиты информации по каналам ПЭМИН и другие*   1. Принципы функционирования и характеристики 2. Защита информации при копировании 3. Защита данных в ноутбуках и на НЖДМ 4. Устройства стирания информации. | | 14 |
| *Самостоятельная работа обучающихся*  Подготовка реферата и презентации по теме: «Анализ возможностей современных антивирусных программ»  Подготовка опорного конспекта «Угрозы исходящие от использования электронной почты»  Подготовка классификационной схемы «Методы борьбы с компьютерными вирусами в Internet» | | 12 |
| **Тема 3.3 Обеспечение информации в операционных системах и приложениях** | Содержание учебного материала | | | **12** | *2,3* |
| Обеспечение безопасности в приложениях MS Word и Excel. Защита информации в БД. Защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. | | |
| Практические занятия  *Обеспечение безопасности в приложениях MS Word и Excel*  *Защита информации в БД на примере MS Access.* | | | 4 |  |
| Семинарские занятия  Тема: *Многоуровневая защита корпоративных сетей*   1. Режим функционирования межсетевых экранов и их основные компоненты. 2. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. 3. Основные схемы сетевой защиты на базе межсетевых экранов. 4. Классы защищенности межсетевых экранов   Тема: *Защита информации в операционных системах и приложениях*   1. Обеспечение информационной безопасности в операционных системах и приложениях. 2. Обеспечение безопасности в приложениях MS Word и Excel. 3. Защита информации в БД.   Тема: *Управление безопасностью*   1. Управление правами пользователей. Привилегии. 2. Ограничение доступа в ПК. Система аудита. 3. Локальная политика безопасности. | | | 7 |
| Контрольная работа по разделу «Методы и средства борьбы с угрозами информационной безопасности» | | | 1 |
| *Самостоятельная работа обучающихся*  Составление сравнительной таблицы «Средства защиты локальных сетей от несанкционированного доступа».  Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов  Выполнение упражнений на обеспечение безопасности в приложениях  Подготовка опорного конспекта «Характеристика современных технических средств защиты информации» | | | 6 |
| **Раздел 4. Современные средства и способы обеспечения информационной безопасности** | | | | **2** |  |
| **Тема 4.1 Современные средства и способы обеспечения информационной безопасности** | Содержание учебного материала | | | **2** | *2* |
| Современные способы и средства негласного получения информации по различным каналам. Современные средства выявления каналов утечки информации. Современные технические средства защиты информации | | |
| Семинарские занятия  Тема: *Современные средства и способы обеспечения информационной безопасности*   1. Современные способы и средства негласного получения информации по различным каналам. 2. Пассивные и активные способы обеспечения информационной безопасности. 3. Современные технические средства защиты информации | | | 2 |  |
| ***Всего:*** | | | | **104** |  |

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);

2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)

3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

**Матрица сопряжения общих и профессиональных компетенций с учебными дисциплинами и профессиональными модулями**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ОК и ПК    Учебные дисциплины и модули | Основы философии | История | Психология общения | Иностранный язык | Физическая культура | Информатика | Элементы математической логики | Теория вероятностей и математическая статистика | Численные методы | Операционные системы | Архитектура компьютерных систем | Технические средства информатизации | Информационные технологии | Основы программирования | Основы экономики | Правовое обеспечение профессиональной деятельности | Теория алгоритмов | Математическое моделирование | Безопасность жизнедеятельности | ПМ.01 | ПМ.02 | ПМ.03 | ПМ.04 | ПМ.05 |
| **ОК 1** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 2** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 3** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 4** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 5** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 6** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 7** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 8** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 9** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ОК 10** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** |  | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** | **\*** |
| **ПК 3.3** |  |  |  |  |  |  |  |  |  |  |  | **\*** |  |  |  | **\*** |  |  | **\*** |  |  | **\*** |  |  |
| **ПК 5.1** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **\*** |  | **\*** | **\*** |  |  |  |  | **\*** |

# **4. условия реализации программы дисциплины**

**4.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы дисциплины требует лаборатории информационно-коммуникационных систем.

Оборудование учебных кабинетов:

посадочные места по количеству обучающихся, рабочее место преподавателя; рабочие программы по МДК, методическая литература; комплект учебной литературы по дисциплине; электронные учебные издания; демонстрационные печатные пособия; экранно-звуковые пособия; электронное сопровождение учебных занятий; дидактический материал по темам; контрольно-измерительные материалы; компьютерные тестовые программы; компьютеры с лицензионным программным обеспечением, принтер, сканеры, телевизор, локальная сеть, комплект учебно-методической документации.

# **4.2. Информационное обеспечение обучения**

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

**Основные источники:**

Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 2013.

**Дополнительные источники:**

1. Защита информации в персональном компьютере: учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ, 2012. – 368с.
2. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов [и др.]. - М. : Горячая линия-Телеком, 2010
3. Куприянов А.И. Основы защиты информации: учебное пособие для студентов высших учебных заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – М.: Издательский центр «Академия», 2011.-256 с.
4. Анисимова И.Н., Стельмашонок Е.В. Защита информации. Учебное пособие. - 2011.

**Интернет-ресурсы:**

<http://www.schoolbase.ru/articles/item/informatikasite>

http://www.intuit.ru/

**Базы данных:**

СПС «Гарант», СПС «Консультант +»

# **5. Контроль и оценка результатов**

# **освоения Дисциплины**

# **Контроль** **и оценка** результатов освоения дисциплины осуществляется преподавателем в процессе проведения семинарских занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

|  |  |
| --- | --- |
| **Результаты обучения**  **(освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
| *Умения:*   * классифицировать основные угрозы безопасности информации; * применять организационные, правовые, программно-технические, криптографические методы и средства защиты информации; * применять антивирусные средства защиты информации. | *Формы контроля:*  Экзамен  *Метод контроля:*  Компьютерное тестирование |
| *Знания:*   * сущность и понятия информационной безопасности; * основные угрозы, методы и средства обеспечения информационной безопасности; * принципы защиты информации от несанкционированного доступа; * правила применения, эксплуатации и обслуживания технических средств защиты информации |