|  |
| --- |
| МИРЭА_ЭМБЛЕМА_приказ |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования  **«Московский технологический университет»**  **МИРЭА** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **УТВЕРЖДАЮ**  Директор Института  Информационных технологий \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.С. Зуев  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г. | **УТВЕРЖДАЮ**  М.П. Романов  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2016 г. | **СОГЛАСОВАНО**  Учебно-методический совет  Института кибернетики  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.С. Хачлаев  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2016 г. |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.В.ОД.11 «БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ»**

Направление подготовки

**09.03.04 «Программная инженерия»**

Программа подготовки

**«Корпоративные информационные системы»**

Квалификация выпускника

**Бакалавр**

Форма обучения

**Очная**

Москва 2017

1. **Цели освоения дисциплины**

Дисциплина «Безопасность функционирования информационных систем» имеет своей целью способствовать формированию у обучающихся профессиональных компетенций ПК–4 ПК – 5, ПК –12 и общекультурные компетенции ОК-7,ОПК-1,ОПК-2 в соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров 09.03.04 Программная инженерияс учетом специфики профиля подготовки – «Корпоративные информационные системы».

1. **Место дисциплины в структуре основной профессиональной образовательной программы (ОПОП) бакалавриата**

Дисциплина «Безопасность функционирования информационных систем» является обязательной дисциплиной базовой части блока Б1.В.ОД.11 «Дисциплины» учебного плана направления подготовки бакалавров 09.03.04 Программная инженерияс учетом специфики профиля подготовки – «Корпоративные информационные системы».

Для освоения дисциплины «обучающиеся должны обладать знаниями, умениями и навыками, полученными в результате формирования и развития компетенций в следующих дисциплинах и практиках:

ПК-4 владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества

Разработка клиент-серверных приложений

Анализ сложности алгоритмов

Основы управления ИТ-проектами

Безопасность функционирования информационных систем

Разработка программного обеспечения для корпоративных информационных систем

Оценка качества информационных систем

Сертификация информационных систем

Информационная безопасность и защита информации

Математические основы защиты информации

Системы электронного документооборота

Мультиагентные информационные системы

Практика по получению профессиональных умений и опыта профессиональной деятельности

ПК– 5 владением стандартами и моделями жизненного цикла

Информационные системы и технологии

Разработка программных приложений

Проектирование информационных систем

Основы управления ИТ-проектами

Безопасность функционирования информационных систем

Качество, стандартизация и сертификация информационных систем

Программная инженерия для корпоративных информационных систем

Корпоративные информационные системы

Интерфейсы информационных систем

Открытые информационные системы

Методы функциональной стандартизации

Основы сопровождения информационных систем

ПК-17 ( способностью использовать технологии разработки объектов профессиональной деятельности в областях: машиностроение, приборостроение, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества):

– процедурное программирование ( 1 семестр);

– объектно-ориентированное программирование (3 семестр);

– технологии программирования ( 1 семестр);

– проектирования информационных систем (1 семестр);

– управление данными ( 1 семестр);

– автоматизация проектирования информационных систем ( 4 семестр);

– интеллектуальные системы и технологии (6 семестр);

– технологии визуализации информации (5 и 6 семестры);

– информационные сети (5 семестр);

– безопасность функционирования информационных систем (7 семестр);

– программная инженерия для корпоративных информационных систем ( 8 семестр);

– проектирование корпоративных информационных систем (1 и 2 семестры);

– информационная безопасность и защита информации ( 6 семестр);

– менеджмент информационных систем (7 семестр);

– аппаратное обеспечение персональных ЭВМ (7 семестр);

– производственная практика (6 и 7 семестры);

– преддипломная практика (8 семестр);

– государственная итоговая аттестация (8 семестр);

ПК-22 (способностью проводить сбор, анализ научно-технической информации, отечественного и зарубежного опытапо тематике исследования):

– иностранный язык (1-4 семестры);

– информационные технологии (2 семестр);

– управление данными ( 2 и 3 семестры);

– технологии визуализации информации (5 и 6 семестры);

– информационные сети (5 семестр);

– безопасность функционирования информационных систем (7 семестр);

– мировые информационные ресурсы (7 семестр);

– информационная безопасность и защита информации (6 семестр);

– корпоративные информационные системы (5 семестр);

– открытые информационные системы (7 семестр);

– информационно-поисковые системы (7 семестр);

– аппаратное обеспечение персональных ЭВМ ( 7семестр);

– учебная практика (2 семестр);

– производственная практика (6 и 7 семестры);

– преддипломная практика ( 8 семестр);

– государственная итоговая аттестация (8 семестр);

ПК–26 **(**способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях):

– управление данными (1 семестр);

– технологии визуализации информации ( 5 и 6 семестры);

– открытые информационные системы (7 семестр);

– менеджмент информационных систем (8 семестр);

– системы электронного документооборота (7 семестр);

– государственная итоговая аттестация (8 семестр);

Элементы данного курса используются при выполнении всех видов практик, при подготовке выпускной квалификационной работы бакалавра и изучении дисциплин "Системы корпоративного управления", "Менеджмент информационных систем", и "Программная инженерия для корпоративных информационных систем", «Основы сопровождения информационных систем».

1. **Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения программы бакалавриата**

**( компетенции выпускников)**

|  |  |
| --- | --- |
| **Формируемые компетенции**  **(код и название компетенции, уровень освоения – при наличии в карте компетенции)** | **Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций** |
| **ПК-4** (способностью проводить выбор исходных данных для проектирования информационных систем, с учетом требования безопасности работы и функционирования) | **Знать –** основные стандарты построения и взаимодействия открытых ИС;  – подходы к интеграции сетей в открытые ИС;  – принципы работы сетевых протоколов и технологий передачи данных в открытых ИС;  – основы организации и функционирования открытых ИС, их стандарты, протоколы и предоставляемые сервисы;  – основные методы и средства реализации удаленных сетевых атак на открытые ИС;  – политики безопасности и меры защиты в открытых ИС;  – комплексный подход к построению эшелонированной защиты для открытых ИС. |
| **Уметь** анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным ИС;  определять и устранять основные угрозы ИБ для открытых ИС;  строить модели угроз и нарушителя ИБ для открытых ИС;  выявлять и устранять уязвимости в основных компонентах открытых ИС;  обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;  проектировать защищенные открытые ИС;  применять стандартные решения для защиты информации в открытых ИС;  используя современные методы и средства, разрабатывать политику ИБ для открытых ИС;  реализовывать системы защиты информации в открытых ИС в соответствии со стандартами по оценке защищенных систем;  применять комплексный подход к обеспечению ИС для ИС;  осуществлять управление и администрирование защищенных ИС. |
| **Владеть** анализом функциональных и нефункциональных требований к ИС, подготовкой частей коммерческого предложения заказчику об объеме и сроках выполнения работ по созданию (модификации) и вводу в эксплуатацию ИС. |
| **ПК-17** (способностью использовать технологии разработки объектов профессиональной деятельности в областях: безопасность информационных систем, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества) | **Знать** основы управления изменениями, основы системного администрирования |
| **Уметь** работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами на исправление несоответствий) , устанавливать права доступа к файлам и папкам |
| **Владеть** проверкой фактического внесения изменений в ИС, определением и назначением необходимого уровня прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС. |
| **ПК-22** (способностью проводить сбор, анализ научно-технической информации, отечественного и зарубежного опытапо тематике исследования безопасности функционирования информационных систем) | **Знать**  предметную область автоматизации, юридические основы взаимоотношений между контрагентами |
| **Уметь** анализировать входную информацию |
| **Владеть** подготовкой технической информации для договоров на выполняемые работы |
| **ПК-26 (**способность оформлять полученные рабочие результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях) | **Знать** инструменты и методы коммуникаций, каналы коммуникаций, модели коммуникаций, технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии, основы управления качеством, инструменты и методы согласования документации, основы менеджмента, в том числе менеджмента качества |
| **Уметь** планировать работы, проводить переговоры, разрабатывать регламентные документы |
| **Владеть** |

1. Содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единицы ( 125,05 ак.часов).

4.1. Распределение объема дисциплины (модуля) по разделам (темам), семестрам, видам учебной работы и формам контроля,

соотнесенным с балльно-рейтинговой системой

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № раздела (темы) | Семестр | Неделя семестра | Объем (в ак. час.) | | | | | | | Формы текущего контроля успеваемости *(по неделям семестра)*  Формы промежуточной аттестации *(по семестрам)* | Макс. количество баллов *(за каждую форму контроля)* |
| Всего | Контактная работа (по видам учебных занятий) | | | | СР | Контроль |
| Всего | **ЛК** | **ЛБ** | ПР |
|  | 7 | 1–2 |  | 12 | 4 | 4 | 4 | 10 | 4 |  |  |
|  | 7 | 3–4 |  | 12 | 4 | 4 | 4 | 10 | 4 |  |  |
|  | 7 | 5–6 |  | 20 | 8 | 8 | 4 | 10 | 4 |  |  |
|  | 7 | 7–8 |  | 16 | 4 | 4 | 8 | 10 | 4 |  |  |
|  | 7 | 9–10 |  | 12 | 4 | 4 | 4 | 10 | 4 |  |  |
|  | 7 | 11–12 |  | 24 | 8 | 8 | 8 | 10 | 8 |  |  |
|  | 7 | 13–14 |  | 20 | 8 | 4 | 8 | 10 | 8 |  |  |
|  | 7 | 15–16 |  | 16 | 4 | 8 | 4 | 10 | 8 |  |  |
| По материалам 7 семестра | | |  | 108 | 36 | 36 | 36 | 80 | 36 | По материалам 7 семестра | 60 |
| **Всего:** | | | ***125*** | ***108*** | ***36*** | ***36*** | ***36*** | **80** | **36** | **Экзамен** | **40** |

4.2. Наименование и содержание разделов дисциплины

|  |  |  |
| --- | --- | --- |
| № раздела | Наименование раздела | Содержание раздела |
| 1 | Безопасность функционирования информационных систем (ИС). Основные понятия. Терминология. | Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний.  Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем.  Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Системообразующие стандарты ISO/IEC.  Формы логической организации стандартов.  Соответствие безопасности информационной системы целевому назначению функциональности. Основные функциональные критерии различных информационных систем. Выделение функциональных критериев для заданной информационной системы. |
| 2 |  | Терминология, основные положения и стандарты теории надежности; факторы, влияющие на характеристики надежности компонентов информационных систем; законы распределения случайных величин, используемых в теории надежности; способы моделирования случайных величин; направления развития и математический аппарат теории надежности; классификацию методов расчета надежности систем; виды испытаний систем на надежность; особенности расчета надежности программного обеспечения (ПО) АС и способы  анализа и обеспечения качества и надежности программных средств (ПС) АС; алгоритмы методов расчета надежности систем; современные методы повышения надежности АС |
| 3 | Концепция, модельное представление и совместимость открытых ИС | Классификация моделей.  Модель ISO OSI. Профили на базе модели ISO OSI. Спецификация POSIX и её развитие. Модель OSE/RM. Тестирование соответствия профилям. Эволюция моделей открытых систем. Модели распределённых вычислений. Модель TOGAF – современная концепция описания компьютерных систем: метод синтеза архитектуры системы, нормативная техническая модель, описание сложной системы специалистами различных предметных областей, информационная база стандартов.  Переносимость и способность к взаимодействию. Базовая модель ИС, её основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы.  Переносимость прикладных программ, данных и пользователей. Способы реализации переносимости.  Расширение базовой модели ИС для взаимодействующих систем. Взаимодействующие системы и распределённая вычислительная система.  Образ единой системы в распределённой вычислительной среде.  Способы реализации способности к взаимодействию. Стек протоколов. Коммуникационный интерфейс. |
| 4 | Системный подход к описанию функциональности на базе модельного представления ИС | Интероперабельность. Стандартизация сервисов. Классификация сервисов платформы приложений. Внутренние сервисы платформы. Сервисы данных. Сервисы человеко-машинного взаимодействия. Сетевые сервисы. Межкатегориальные сервисы.  Основные классы прикладных программ. |
| 5 | Методологические основы распределённой обработки и хранения данных и коммуникационная инфраструктура открытых ИС | Уровни распределения обработки данных в архитектуре ИС. Модели организации распределённых вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Модель RM-ODP. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки: диспетчеризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок.  Проводные, оптические, радиоканалы.  Эффективное кодирование, помехоустойчивость, управление линией передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay. |
| 6 | Критерии безопасности функционирования информационных систем. | Понятие функционального критерия качества функционирования информационных систем. Критерии (сложность, корректность, трудоемкость) на этапах проектирования информационных систем. Безопасность функционирования этапа эксплуатации информационных систем (критерии: сложность, надежность, эффективность). Критерии этапа сопровождения информационных систем (модифицируемость, мобильность, трудоемкость). |
| 7 | Интранет, как открытая система, ее уязвимости и информационные ресурсы как объекты атак | Понятие сети Интранет как примера открытой системы и задачи ее защиты. Структура Интранет. Эталонная модель Интранет. Экстранет. Порталы: виды порталов, схема, компоненты, базовые сервисы. Корпоративные порталы.  Уязвимость архитектуры клиент-сервер: конфигурация системы, уязвимость операционных систем, уязвимость серверов (уязвимость систем управления базами данных, уязвимость систем электронного документооборота), уязвимость рабочих станций, уязвимость каналов связи (перехват паролей, перехват незащищенного трафика, недостатки протоколов, уязвимости каналообразующего оборудования). Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX, …) и ошибки в программном обеспечении. Сетевые вирусы. Виды угроз ресурсам интранета и Интернета.  Уровни информационной инфраструктуры. |
| 8 | Безопасность функционирования сетей хранения данных | Архитектура распределённого хранения данных. Сети хранения данных (SAN – Storage Area Networks). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN. Концепция глобальной коммуникационной инфраструктуры. |
| 9 | Возможные методики аудита безопасности корпоративных и распределенных ИС | Новое поколение стандартов безопасности  Стандарты ISO/IEC 17799:2000 (BS 7799-1:2000) и BS 7799-2:2000, Стандарт COBIT 3rd Edition,  Стандарт ISO/IEC 15408 |

4.3. Лабораторные работы (ЛБ)

Лабораторная работа 1. Знакомство с организацией и работой открытых сетей (на примере Интернета), их протоколами и сервисами.

Лабораторная работа 2. Изучение уязвимостей некоторых сервисов и протоколов. Поиск информации по уязвимостям в Интернете. Способы повышения безопасности функционирования.

Лабораторная работа 3. Организация безопасности функционирования корпоративной информационной системы при использовании защищенных версий операционной системы Windows.

Лабораторная работа 4. Организация безопасности функционирования корпоративной информационной системы при использовании защищенных версий операционной системыОС Linux.

Лабораторная работа 5. Основные сетевые утилиты ОС Linux, используемые для сбора информации об атакуемой системе. Программа для сканирования и исследования сетевой безопасности nmap.

Лабораторная работа 6. Изучение безопасности функционирования и настройки межсетевых экранов на примере netfiler/iptables.

Лабораторная работа 7. Изучение безопасности функционирования корпоративной информационной системы при работе шифрующей файловой системы и протокола удалённого управления.

Лабораторная работы 8. Оценка безопасности функционирования и оценка влияния на корпоративную информационную систему DLP-системы.

4.4. Практические занятия (ПР)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | № раздела дисциплины | Тематика практических занятий | Трудоемкость (в часах) |
| 1 | 1 | Общая постановка задачи оценки безопасности функционирования Задачи организации безопасности функционирования информационной системы. Сравнение различных абстрактных моделей безопасности функционирования для одной КИС. Повтор навыков оценки ИС по эталонной модели OSI. | 4 |
| 2 | 2 | Дефектологические свойства информационных систем. Изучение различных дефектов информационных систем. Рассмотрение свойств дефектогенности, дефектабельности и дефектоскопичности информационных систем в зависимости от свойств системы. | 4 |
| 3 | 3 | Стандарты управления информационных систем. Ознакомление с общими положениями нормативных документов. Ознакомление с процедурами стандартизации и сертификации информационной системы. | 4 |
| 4 | 4,5 | Метрики информационных систем. Исследование различных информационных систем, определение их функциональных критериев. Отличия функциональных критериев для различных систем одного класса. Понятия монитора безопасности субъектов и изолированной программной среды информационной системы. | 8 |
| 5 | 5 | Критерии web-порталов, сайтов, ПО и сетевого программного обеспечения. Характеристики безопасного функционирования информационных систем, понятия субъект и объект в ИС. | 4 |
| 6 | 6 | Критерии безопасности функционирования информационных систем. Исследование различных информационных систем, выявление их критериев качества. Методы обеспечения безопасного функционирования информационных систем.Угрозы безопасности функционирования информационных систем. | 8 |
| 7 | 7 | Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Классификация отказов информационной системы. Угрозы анализа сетевого трафика и подмены объекта или субъекта информационных систем. Политики безопасности информационных систем. | 8 |
| 8 | 8,9 | Сети хранения данных (SAN – Storage Area Networks). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN. Концепция глобальной коммуникационной инфраструктуры. Системы обнаружения атак на информационную систему и контент-анализа. Контроль конфиденциальности объектов функционирующих информационных систем. Контроль целостности объектов функционирующих информационных систем. | 4 |
| Всего в 7 семестре: | | | 36 |
| **Всего:** | | | **36** |

1. **Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине**

Виды самостоятельной работы обучающегося, порядок и сроки ее выполнения:

* выполнение курсового проекта;
* подготовка к лекциям, лабораторным работам и практическим занятиям с использованием конспекта лекций, материалов практических занятий и приведенных ниже (п.7) источников (в течение 7-го семестра в соответствии с расписанием занятий);

Перечень вопросов для проведения текущего контроля и промежуточной аттестации – в соответствии с тематикой разделов дисциплины.

1. **Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине**

6.2. Критерии и шкалы оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.

**В отдельном файле**

**7. Ресурсное обеспечение дисциплины**

7.1. Основная и дополнительная учебная литература, необходимая для освоения дисциплины

а) основная литература:

1. Голицына О.Л., Партыка Т.Л, И.И. Попов «Программное обеспечение» 3-е издание ФОРУМ 2010 г.

2. Максимов Н.В., Попов И.И. «Компьютерные сети» учебное пособие для студентов учреждений профессионального образования ФОРУМ, 2010 г.

3. Креопалов В. В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. -М.: Изд. центр ЕА-ОИ, 2011.-278 с. <http://www.biblioclub.ru/book/90753>

4.Федорова Г.Н. Информационные системы, учебник, 3 издание, М. Издательский центр «Академия», 2013г.

б) дополнительная литература:

1. Хорев П.Б.. Программно-аппаратная защита информации. М.: ФОРУМ, 2011.
2. **Платонов В.В.** Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. М.: Издательский центр «Академия», 2010.
3. Хорев П.Б. Криптографические интерфейсы и их использование. М.: Горячая линия-Телеком, 2011.
4. Семененко В.А., Федоров Н.В. Программно-аппаратная защита информации. М.: Издательство МГИУ, 2010.
5. Гришина Н.В. Комплексная система защиты информации на предприятии. М.: Форум, 2010.
6. Хорев П.Б. Объектно-ориентированное программирование. М.: Издательский центр «Академия», 2011.
7. Зыков О.В Основы проектирования корпоративных информационных систем, М.Издательский дом высшей школы экономики, 2012г.

7.2. Ресурсы информационно-телекоммуникационной сети Интернет, необходимые для освоения дисциплины:

1. <http://www.intuit.ru/>;
2. Справочные системы и сайты поддержки Oracle, демоверсии систем MRP I, CRP, MRP II и т.д*.*
3. Электронный ресурс, ЭБС «КнигаФонд», <http://www.knigafund.ru/sections/165>
4. Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) — электронная библиотека по всем отраслям знаний, <http://www.iprbookshop.ru/3-texnika.-texnicheskie-nauki.html>.
5. Comodo Internet Security Rus 2015 (8.2.0.4703), источник – Free
6. Microsoft Security Essentials 4.7.205.0, источник – Free
7. Microsoft Network Monitor 3.4 источник – Free
8. TeamViewer 10.0.47484 источник – Free
9. FileZilla 3.14.1 источник – Free
10. Remote Administrator 3.0 Лицензионный сертификат Famatech от 26.03.2008г. – бессрочно
11. Ontrack EASYRecovery 6.10.07 источник – Free.

7.3. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В процессе выполнения практических и лабораторных работ необходимо следующее:

* операционная система – Windows XP,7,8;
* программное обеспечение Microsoft Office.

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

* учебная аудитория, оснащенная презентационным оборудованием.
* лекционная аудитория должна быть оснащена презентационным оборудованием (персональный компьютер, мультимедийный проектор, экран, программа для создания и проведения презентаций, например, Microsoft Office PowerPoint).

2. Компьютерные классы для проведения групповых занятий с применением активных и интерактивных технологий и самостоятельной работы студентов, включающие в себя:

* 25 ПЭВМ (Микропроцессор Intel Pentium 4 2,8GHz, память 1Гб (оперативная) и 250Гб (винчестер), дисковод СD-DVD R/RW, встроенная звуковая карта, видео – Nvidia GeForce 7300LE 256Мб);
* Принтер HP LJP1102 – 1 шт;
* МФУ HP LJM1120 – 1 шт.

Минимальные требования к компьютеру:

|  |  |
| --- | --- |
| Компонент | Требования |
| Процессор | Компьютер с процессором Pentium с тактовой частотой не ниже 1 ГГц. |
| Операционная система | * Microsoft Windows 7 или более поздняя версия * Microsoft Windows XP или более поздняя версия * Microsoft Windows 2000 с пакетом обновления 3 (SP3) или более поздним. * ОС Linux.   Пакет программ Microsoft Office 2007/2010.  Системы программирования Microsoft Visual Studio и Borland Developer Studio.  Персональный межсетевой экран VipNet Personal Firewall.  Интернет ресурсы:  www.fstec.ru; www.security.ru; www.infosec.ru; catalog.sec.ru. |
| Память | Не менее 512 МБ оперативной памяти. |
| Дисковое пространство | Для установки Microsoft Office 2003 необходимо 8 ГБ свободного места на жестком диске. |
| Монитор | Необходим монитор Super VGA с разрешением 800x600 или более высоким, отображающий 256 и более цветов. |

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.04 «Программная инженерия» с профилем «Корпоративные информационные системы».

Автор (ы):

к.т.н. доцент кафедры корпоративных информационных систем \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ АА. Башлыкова

Рабочая программа дисциплины одобрена на заседании кафедры корпоративных информационных систем

(протокол № 1 от 30 августа 2017 г.)

Заведующий кафедрой

корпоративных информационных систем \_\_\_\_\_\_\_\_\_\_\_\_\_ А.Б. Петров