ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

Кафедра «Информационные технологии и защита информации»
Кафедра «Естественнонаучные дисциплины»

УТВЕРЖДАЮ:
Проректор по научной работе
и международным связям
_____ С.В. Бушуев
«27» февраля 2017 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ В АСПИРАНТУРУ

по направлению подготовки
10.06.01 Информационная безопасность
направленность
«Методы и системы защиты информации, информационная безопасность»

Форма обучения – очная

Разработчик _____ к.т.н., Т.Ю. Зырянова

Начальник отдела Д и А _____ д.т.н., Н.Ф. Сирина

Екатеринбург
2017

Введение

Содержание программы сформировано на основе ФГОС ВО по программам специалитета и магистратуры (п. 40 «Порядка приема на обучение по образовательным программам ВО – программам подготовки научно-педагогических кадров в аспирантуре»).

1. Теория информационной безопасности и методология защиты информации

Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Методы обеспечения информационной безопасности Российской Федерации. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации. Организационная основа системы обеспечения информационной безопасности российской федерации. Основные элементы организационной системы обеспечения информационной безопасности Российской Федерации. Основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Информация как объект правовых отношений. Обладатель информации. Право на доступ к информации. Ограничение доступа к информации. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации. Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки угроз. Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Понятие политики безопасности, технология создания и внедрения. Дискреционный принцип доступа. Классификация субъектов и объектов доступа. Требования к механизмам разграничения доступа. Модель дискреционного доступа.

2. Правовые основы обеспечения информационной безопасности

Назначение и структура правового обеспечения защиты информации. Информационное право. Принципы информационного права. Система информационного права. Методы правового регулирования в области информационной безопасности. Государственная политика обеспечения информационной безопасности. Структура органов защиты информации. Структура нормативных правовых актов Российской Федерации в области защиты информации. Построение системы управления деятельностью по защите государственной тайны на предприятии. Нормативно-правовые акты. Определение предмета защиты. Лицензирование деятельности в области защиты государственной тайны. Допуск граждан и должностных лиц к государственной тайне. Перечень сведений конфиденциального характера. Виды информационных ресурсов по категориям доступа. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации. Защита сведений, составляющих коммерческую тайну. Секрет производства (ноу-хау). Защита сведений, составляющих служебную тайну. Подтверждение соответствия. Формы подтверждения соответствия. Добровольное подтверждение соответствия. Обязательное подтверждение соответствия. Сертификация. Сертификация средств защиты информации. Система сертификации средств защиты информации, составляющей государственную тайну. Нормативно-правовые основы, лицензионные требования и условия, а также основы организационно-технических мероприятий по технической защите информации, проводимые в федеральных органах исполнительной власти, органах исполнительной власти субъектов федерации, местного самоуправления, на предприятиях оборонно-промышленного комплекса, организационной структуры государственной системы противодействия техническим разведкам и технической защиты информации, задач и функций уполномоченных в области лицензионной деятельности федеральных органов исполнительной власти, сети испытательных и аккредитационных центров. Методы, методики и исполнение установленных механизмов и организационных процедур лицензирования деятельности в области технической защиты информации. Организационно-правовые основы технической защиты информации ограниченного доступа в отрасли, на предприятии, в учреждении, организации. Планирование и организация работ по технической защите информации ограниченного доступа в отрасли, на предприятии, в учреждении, организации.

3. Техническая защита информации

Понятие об информации как о предмете защиты. Основные свойства информации как предмета защиты. Категории информации. Информация как

товар. Копирование (тиражирование) информации. Виды защищаемой информации. Демаскирующие признаки. Видовые демаскирующие признаки. Демаскирующие признаки сигналов. Основные задачи инженерно-технической защиты информации. Особенности инженерно-технической защиты информации. Выбор рационального состава средств и систем технической защиты информации для защиты информации на конкретном объекте информатизации в конкретных условиях эксплуатации. Выполнение методов и процедур выявления угроз безопасности информации на предприятии. Порядок осуществления работ по технической защите информации на предприятии (в организации, учреждении) на различных этапах жизненного никла объекта информатизации. Оценка состояния технической защиты информации на предприятии (организации, учреждении).

4. Безопасность вычислительных сетей

Основные положения для планирования безопасной сети. Многоуровневый подход к обеспечению информационной безопасности. Подсистема защиты от несанкционированного доступа. Подсистема криптографической защиты. Подсистема управления идентификацией и доступом. Подсистема безопасности коммутируемой инфраструктуры и беспроводных сетей. Подсистема управления средствами защиты информации. Подсистема контроля информационных ресурсов. Подсистема межсетевого экранирования. Подсистема обнаружения и предотвращения вторжений. Подсистемы защиты от вредоносных программ и спама. Подсистема контроля эффективной защиты информации. Подсистема мониторинга и управления инцидентами информационной безопасности. Подсистема обеспечения непрерывности функционирования средств защиты. Основы сетевого и межсетевого взаимодействия. Информационная безопасность при сетевом и межсетевом взаимодействии. Компьютерные вирусы. Файловые вирусы. Макровирусы. Загрузочные вирусы. Методы защиты от обнаружения. Троянские кони. Сетевые черви. Потайные ходы. Руткиты. Вредоносные программы для мобильных устройств. Прочие вредоносные программы. Элементы защиты от вредоносного программного обеспечения. Сетевые атаки. Атаки «отказ в обслуживании». Распределенные атаки «отказ в обслуживание». Распределенные рефлекторные атаки «отказ в обслуживании». Таксономия атак «отказ в обслуживании» и защитных механизмов. Классификация атак с точки зрения цели атаки. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

5. Программно-аппаратная защита информации

Задачи аутентификации. Факторы аутентификации. Парольная аутентификация. Аутентификация на основе открытого пароля. Аутентификация на основе хешированного пароля. Аутентификация на основе PIN-кода. Парольные политики. Недостатки методов аутентификации с запоминаемым паролем. Аутентификация с помощью биометрических характеристик. Недостатки методов аутентификации с запоминаемым паролем. Аутентификация с помощью одноразовых паролей. Методы аутентификации с помощью OTP-токенов. Метод «Запрос-ответ». Метод «только ответ». Технология межсетевых экранов. Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояний. Межсетевые экраны уровня ядра. Новое поколение межсетевых экранов. Протокол IPSec. Правила безопасности подключений. Сопоставление безопасности. Создание подключения IPSec. Протокол обмена интернет-ключами. Виртуальные частные сети. Туннелирование. Протоколы VPN канального уровня. Основные виды защищенных связей. Протоколы VPN транспортного уровня.

6. Безопасность систем баз данных

Понятия и определения реляционной модели данных. Проектирование реляционных баз данных. Манипулирование реляционными базами данных, реляционная алгебра. Особенности логической архитектуры современных реляционных баз данных. Технологии и модели клиент-серверной архитектуры. Теоретические основы безопасности баз данных и СУБД. Понятие безопасности баз данных. Угрозы безопасности баз данных. Меры защиты баз данных и СУБД. Механизмы и методы обеспечения целостности информации в реляционных базах данных. Обработка транзакций. Управление параллельностью работы транзакций. Реализация ограничений в базах данных. Механизмы и методы обеспечения конфиденциальности информации в реляционных базах данных. Защита от несанкционированного доступа пользователей к объектам баз данных и сервисам СУБД. Использование криптографических методов защиты информации в системах баз данных. Защита баз данных от «внедрения в SQL». Механизмы и методы обеспечения доступности информации в реляционных базах данных. Резервное копирование и восстановление баз данных. Резервирование серверов СУБД. Верификация баз данных и проведение аудита в СУБД. Методы и средства верификации баз данных. Активный аудит систем баз данных. Программа ISS Database Scanner. Мониторинг активности пользователей на уровне СУБД. Организация местного аудита в базах данных с использованием триггеров.

7. Управление информационной безопасностью

Определение системы управления информационной безопасностью (СУИБ). Среда функционирования СУИБ. Функциональные составляющие СУИБ. Стандартизация СУИБ. Понятия типизации и стандартизации. Стандарты серии ГОСТ Р ИСО/МЭК 15408. Стандарты серии ГОСТ Р ИСО/МЭК 27000. Функциональные составляющие СУИБ. Управление процессами функционирования системы защиты информации. Организационно-правовая составляющая системы защиты информации. Программно-техническая составляющая системы защиты информации. Экономическая составляющая системы защиты информации. Методологические основы управления информационными рисками. Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Измерение рисков. Выбор допустимого уровня риска. Выбор контрмер и оценка их эффективности. Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков. Табличные методы оценки рисков.

8. Экономика защиты информации

Информация как товар. Информация фирмы. Информация как важнейший ресурс экономики. Стадии жизненного цикла новой техники. Основные экономические принципы и методы защиты информации. Страхование информационных рисков. Процедура страхования информационных рисков. Стоимость страхования. Интеллектуальная собственность предприятия и предпринимательский риск. Экономическая оценка объектов интеллектуальной собственности. Предпринимательский риск и методы его снижения. Сущность себестоимости продукции. Сущность и виды себестоимости, способы расчета. Экономическая сущность расчета себестоимости. Особенности определения себестоимости программных средств. Особенности установки цен на информационные услуги. Методы ценообразования. Экономическая эффективность защиты информации. Теоретические аспекты определения показателей экономической эффективности. Оценка сравнительной экономической эффективности от внедрения средств защиты информации.

9. Комплексная система защиты информации (КСЗИ)

Определение системы защиты информации. Среда функционирования системы защиты информации. Функциональные составляющие системы защиты информации. Управление процессами функционирования КСЗИ. Модель управления системой защиты информации. Планирование защиты

информации. Оперативное управление системой защиты информации. Календарно-плановое руководство. Принципы комплексной защиты корпоративной информации. Архитектура корпоративной информационной системы. Структура системы защиты информации в корпоративной информационной системе. Комплексный подход к обеспечению информационной безопасности корпоративных информационных систем. Подсистемы информационной безопасности корпоративных информационных систем. Подсистема защиты информации от несанкционированного доступа. Подсистема криптографической защиты. Подсистема управления идентификацией и доступом. Подсистема обеспечения безопасности коммутируемой инфраструктуры и беспроводных сетей. Подсистема управления средствами защиты информации. Подсистема контроля использования информационных ресурсов. Подсистема контроля эффективности защиты информации. Подсистема мониторинга и управления инцидентами информационной безопасности. Подсистема обеспечения непрерывности функционирования средств защиты.

10. Криптографическая защита информации

Предмет криптографии и основные определения. Математические основы криптографии. Математическая модель шифра. Классификация шифров. Обзор истории криптографии. Симметричные криптосистемы. Шифры подстановок и перестановок. Понятие подстановки. Математическая модель шифра подстановок. Сравнимость. Примеры классических шифров подстановок. Математическая модель шифра перестановок. Маршрутные перестановки как пример шифра перестановок. Математическая модель шифра замены. Классификация шифров замены. Поточные шифры. Принципы построения поточных шифров. Линейные регистры сдвига. Пример поточного шифрования. Блочные шифры. Принципы построения блочных шифров. Стандарт симметричного шифрования DES. Алгоритм Rijndael. Алгоритм ГОСТ 28147-89. Подтверждение целостности информации криптографическими средствами. Обеспечение целостности информации при передаче и хранении. Хэш-функции. Алгоритмы вычисления хэш-значений. Подтверждение подлинности источника информации криптографическими средствами. Понятие электронной подписи. Алгоритм электронной подписи на основе алгоритма RSA. Алгоритм электронной подписи на основе эллиптических кривых. Управление ключами. Задачи управления ключами. Генерация ключей. Хранение ключей. Распределение ключей. Алгоритм Диффи-Хеллмена.

ЛИТЕРАТУРА

Основная литература

1. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 г. N 6-ФКЗ и от 30 декабря 2008 г. N 7-ФКЗ).
2. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ (в ред. от 21 июля 2011 г. № 252-ФЗ).
4. Федеральный закон «О государственной тайне» от 21 июля 1993 года № 5485-I (в ред. от 08.11.2011 N 309-ФЗ.
5. Федеральный закон «О коммерческой тайне » от 18.12.2006 №231-ФЗ.
6. Федеральный закон «О лицензировании отдельных видов деятельности» от мая 2011 года N 99-ФЗ (в ред. от 28.07.2012г. №133-ФЗ).
7. Федеральный закон «О персональных данных » от 27 июля 2006 г. № 149-ФЗ.
8. Доктрина информационной безопасности Российской Федерации (Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895).
9. Постановление Правительства Российской Федерации «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне от 06 февраля 2010г. № 63.
10. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (в ред. от 31.03.2010 № 200, от 24.09.2010 № 749).
11. Постановление Правительства Российской Федерации от 1 ноября 2012г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
12. Постановление Правительства Российской Федерации от 26.06.1995 №608 (ред. от 21.04.2010 г.) «О сертификации средств защиты информации».
13. Постановление Правительства Российской Федерации от 29 декабря 2007г. №957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».
14. Постановление Правительства Российской Федерации от 17 ноября 2007г. № 781 «Об утверждении Положения об обеспечении

безопасности персональных данных при их обработке в информационных системах персональных данных».

15. Постановление Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

16. Указ Президента Российской Федерации от 6 марта 1997 года № 188 (в ред. от 23.09.2005 №1111) «Об утверждении Перечня сведений конфиденциального характера».

17. Методический документ «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных». Утвержден руководством 8 Центра ФСБ России 21 февраля 2008г. №149/6/6-622.

18. Руководящий документ Гостехкомиссии Российской Федерации «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации».

19. Руководящий документ Гостехкомиссии Российской Федерации «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

20. Руководящий документ Гостехкомиссии Российской Федерации «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации».

21. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

22. ГОСТ 34.601-89 «Информационная технология. Стадии создания автоматизированных систем».

23. ГОСТ Р 34.602-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

24. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

25. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

26. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

27. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

28. ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности»

29. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. М.: Изд-во «Солон-Пресс, 2009. – 256 с.

30. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др. – М.: Горячая Линия - Телеком, 2012. – 497 с.

31. Грибунин, В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин. – М.: Издательский центр «Академия», 2009. - 416 с.

32. Домарев, В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД ДС», 2008.

33. Зайцев, А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещаряков и др. - М.:ООО «Издательство Машиностроение», 2009 -508 с.

34. Кокшаров, В.А. Экономика организаций. Учебно-методическое пособие / В.А. Кокшаров. – Екатеринбург: Изд-во УрГУПС, 2011. – 63 с.

35. Орин, Т. Администрирование корпоративных сетей на основе Windows Server 2008 / Т. Орин, Д. Поличелли, Й. Маклин, Дж. К. Макин, П. Менкьюзо, Д.Р. Миллер. – М.: Русская редакция, 2011. – 504 с.

36. Паршина, Е.В. Проектирование информационных систем. Конспект лекций / Е.В. Паршина, К.А. Паршин. – Изд-во УрГУПС, 2010.

37. Платонов, В.В. Программно-аппаратные средства защиты информации / В.В. Платонов. – М.: Академия, 2013. – 396 с.

38. Смагин, А.А. Базовые принципы информационной безопасности вычислительных систем / А.А. Смагин. – Ульяновск.: Ульяновский государственный технический университет, 2009. – 168 с.

39. Таненбаум, Э. Компьютерные сети / Э. Таненбаум. – Санкт-Петербург: Питер, 2011. – 991с.

40. Торокин, А.А. Инженерно-техническая защита информации (учеб.пособие для студентов, обучающихся по специальностям в обл. информ.безопасности) / А.А. Торокин.- М.: Изд-о Гелиос АРВ, 2008.-960 с.

41. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Академия, 2009. – 272 с.

42. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

43. Шепитько, Г.Е. Экономика защиты информации / Г.Е. Шепитько. – Изд-во «Москва», 2011. – 64 с.

Дополнительная литература

1. Гражданский Кодекс РФ: часть 1 от 30.11.1994 N 51-ФЗ (ред. от 30.11.2011); часть 2 от 26.01.1996 N 14-ФЗ (ред. от 30.11.2011); часть 3 от 26.11.2001 N 146-ФЗ (ред. от 30.06.2008); часть 4 от 18.12.2006 N 230-ФЗ (ред. от 08.12.2011).

2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ (в ред. от 6 декабря 2011 г. N 404-ФЗ).

3. Уголовный кодекс Российской Федерации от 24 мая 1996 г. № 63-ФЗ (в ред. от 07.12.2011 N 420-ФЗ).

4. Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 21 июля 1997г. №119-ФЗ.

5. Федеральный закон «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» от 15 августа 1996 г. № 114-ФЗ (в ред. от 6 декабря 2011 г. N 397-ФЗ).

6. Федеральный закон «О техническом регулировании» от 27.12.2002 №184-ФЗ (в ред. от 28.07.2012).

7. Федеральный закон «О Федеральной службе безопасности» от 3 апреля 1995 г. № 40-ФЗ (в ред. от 27 июля 2010 г. N 238-ФЗ).

8. Положение о межведомственной комиссии по защите государственной тайны (в ред. Указов Президента РФ от 26.02.2009 N 228, от 14.02.2012 N 183).

9. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Приказом Гостехкомиссии РФ от 27.10.1995г. №199).

10. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией РФ 25.11.1994 г.).

11. Постановление Правительства РФ от 3 ноября 1994г.№1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

12. Приказ ФСБ РФ от 13.11.1999 N 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия» (Зарегистрировано в Минюсте РФ 27.12.1999г. №2028).

13.Приказ Министерства культуры и массовых коммуникаций Российской Федерации от 8 ноября 2005г. № 536 «О Типовой инструкции по делопроизводству в федеральных органах исполнительной власти».

14.Указ Президента Российской Федерации «Вопросы Федеральной службы по техническому и экспортному контролю» от 16 августа 2004 года № 1085 (в ред. от 23.10.2008г. №1517).

15.Руководящий документ Гостехкомиссии Российской Федерации «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

16.ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов».

17.ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения».

18.ГОСТ 34.603 - 92 «Информационная технология виды испытаний автоматизированных систем».

19.ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

20.Приказ ОАО «РЖД» от 27 декабря 2004г. №240 «О порядке обращения с информацией, составляющей коммерческую тайну, в ОАО «РЖД» (в ред. Приказа ОАО «РЖД» от 19.11.2006 №267).

21.Грабер, М. Введение в SQL / М. Грабер. – М.:Лори, 2010. – 228 с.

22.Гугуева, Т.А. Конфиденциальное делопроизводство: Учебное пособие / Т.А. Гугуева. – М.: Изд.: Альфа-М, 2012г.

23.Диго, С.М. Базы данных. Проектирование и создание / С.М. Диго. - М:. Изд. центр ЕАОИ, 2008. – 172 с.

24.Загинайлов, Ю.Н. Комплексная система защиты информации на предприятии. Учебно-методическое пособие / Ю.Н. Загинайлов и др. - Барнаул: АлтГТУ, 2010. – 287 с.

25.Кришталюк, А.Н. Конфиденциальное делопроизводство и защита коммерческой тайны. Учебно-методическое пособие / А.Н. Кришталюк. - г. Орел, 2011г.

26.Кудрявцев, К.Я. Создание баз данных / К.Я. Кудрявцев. – М.: НИЯУ МИФИ, 2010. – 155 с.

27.Кузин, А.В. Базы данных / А.В. Кузин, С.В. Левонисова. – М.: Академия, 2008.

28.Панасенко, С. Алгоритмы шифрования. Специальный справочник / С. Панасенко. Спб: БХВ-Петербург, 2009.

29.Токмаков, Г.П. Базы данных. Концепция баз данных, реляционная модель данных, языки SQL и XML / Г.П. Токмаков. – УлГТУ, 2010. – 193 с.

30.Черенев, Ю.Б. Пожарно-охранная сигнализация: сб. лабораторных работ / Ю.Б. Черенев. - Екатеринбург: Изд-во УрГУПС, 2010. – 48 с.

31.Черенев, Ю.Б. Видеоохранные системы: практикум / Ю.Б. Черенев. – Екатеринбург: Изд-во УрГУПС, 2009. – 48 с.

Программное обеспечение и Интернет–ресурсы

1. http://www.fstec.ru – Федеральная служба по техническому и экспортному контролю Российской Федерации.
2. http://www.inside-zi.ru – Информационно-методический журнал «Защита информации. Инсайд».
3. http://www.jetinfo.ru – Информационный бюллетень «Jet Info».
4. http://citforum.ru – «Сервер Информационных Технологий».
5. http://www.iso27000.ru – Интернет-портал «ISO27000.RU».