МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан ФЭМИТ
_____ С. А. Баркалов
«_____»_____**2018 г.**

РАБОЧАЯ ПРОГРАММА
дисциплины

«Средства защиты информации в интегрированных технических системах управления»

Направление подготовки (специальность) 27.04.04 - Управление в технических системах

Профиль (Специализация) Системы и средства автоматизации технологических процессов в строительстве

Квалификация (степень) выпускника магистр

Нормативный срок обучения 2 года

Форма обучения очная

Автор программы: д.т.н., проф. _____ Коптиков В. П.

Программа обсуждена на заседании кафедры автоматизации технологических процессов и производств
«30»__08__2018 года Протокол № 1

Зав. кафедрой_____ к.т.н., доц. Белоусов В. Е.

Воронеж 2018

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. **Цели дисциплины** изучение комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности, их информационных ресурсов.

1.2. Задачи освоения дисциплины: овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения. Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина Б1.В.ОД.5 « Средства защиты информации в интегрированных технических системах управления» относится к обязательным дисциплинам вариативной части учебного плана.

В результате изучения дисциплины студенты должны иметь общее представление о методах обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты, функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов . Полученные знания и навыки могут применяться в процессе подготовки магистерской диссертации.

Таким образом, «Функциональный анализ технической системой при алгоритмизации управления» использует знания и навыки, полученные при изучении дисциплины «Компьютерные технологии управления в технических системах», «Информационное обеспечение систем управления на основе SCADA программ», «Применение CALS/ИПИ технологий в технических системах».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс изучения дисциплины «Средства защиты информации в интегрированных технических системах управления» направлен на формирование следующих компетенций:

- готовностью к активному общению с коллегами в научной, производственной и социально-общественной сферах деятельности (ОК-3)
- способностью самостоятельно приобретать и использовать в практической деятельности новые знания и умения в своей предметной области (ОПК-4);
- способностью использовать современные технологии обработки информации, современные технические средства управления, вычислительную технику, технологии компьютерных сетей и телекоммуникаций при проектировании систем автоматизации и управления (ПК-10);
- способностью разрабатывать и применять современные технологии создания программных комплексов (ПК-13)
- готовностью участвовать в поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ПК-18).

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Средства защиты информации в интегрированных технических системах управления» составляет _4_ зачетных единицы, 144 часов.

Вид учебной работы	Всего часов	Семестры
		3
Аудиторные занятия (всего)	44	44
В том числе:		
Лекции	22	22
Практические занятия (ПЗ)	22	22
Лабораторные работы (ЛР)		
Самостоятельная работа (всего)	100	100
В том числе:		
Курсовой проект		+
Расчетно-графическая работа / Контрольная работа (количество)		
Вид промежуточной аттестации (зачет, экзамен)		Зачет
Общая трудоемкость час	144	144
зач. Ед.	4	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Основные термины и определения. Классификация защищаемой информации . Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов «О стратегии национальной безопасности Российской федерации до 2020 года» и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов Российской Федерации в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа. Проблемы региональной информационной безопасности .
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	. Стандарты по оценке защищенных систем. Критерии безопасности компьютерных систем. Европейские «Критерии безопасности информационных технологий». Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Обзор серии стандартов ISO/IEC 17799. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Стандарт ISO/IEC 27001. Российский стандарт ГОСТ Р ИСО/МЭК 27001-2006. Стандарты ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408. Российская классификация средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК
3	Абстрактные модели обеспечения информационной безопасности	Ранние модели управления доступом. . Модель матрицы доступов Харрисона – Руззо – Ульмана. Модель Белла и Лападула. Модель систем военных сообщений. Понятие контроля доступа, базирующегося на ролях
4	Основные угрозы информационной безопасности	Анализ и классификация угроз информационной безопасности автоматизированных систем. Причины, виды,

	автоматизированных систем	каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы, основанные на информационных сетевых атаках
5	Основы построения систем защиты информации	Основные принципы обеспечения информационной безопасности в АС. Основные методы и средства защиты информации. Порядок построения защищенной автоматизированных системах управления (АС). Аттестация объектов информатизации по требованиям безопасности информации
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	Проблемы обеспечения информационной безопасности в АС. Основные термины и определения. Основные угрозы безопасности АС. Правовые основы защиты информации. Цели защиты информации. Режимы защиты информации. Классификация компьютерных преступлений

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин				
		1	2	3	4	5
1	Компьютерные технологии управления в технических системах	+			+	+
2.	Информационное обеспечение систем управления на основе SCADA программ	+	+	+	+	
3	Применение CALS/ИПИ технологий в технических системах		+		+	+

5.3. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Лаб. Зан.	Практ. Зан.	СРС	Все-го час.
1	Информационная безопасность в системе национальной безопасности Российской Федерации	2		2	16	20
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	4		4	16	24
3	Абстрактные модели обеспечения информационной безопасности	4		4	16	24
4	Основные угрозы информационной безопасности автоматизированных систем	4		4	16	24
5	Основы построения систем защиты информации	4		4	16	24
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	4		4	20	28

5.4. Практические занятия

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудо-емкость (час)
1.	1	Математические аспекты применения формальных моделей	2
2	2	Практическая реализация и оценка формальных моделей	4
3	3	Исследование корректности систем защиты	4
4	4	Инсталляция и настройка штатных средств операционных систем, предназначенных для защиты от НСД и программно-аппаратных комплексов защиты от НСД	4
5	5	Инсталляция и настройка МЭ, программно-аппаратных средств защиты информации при передаче по открытым каналам связи и разграничения доступа к сетевым ресурсам	4
6	6	Анализ состояния информационных систем и организация защиты от хакерских атак	4

5.5.Лабораторные работы

Лабораторные работы не предусмотрены

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ, КУРСОВЫХ И КОНТРОЛЬНЫХ РАБОТ

Курсовой проект предусмотрен в 3 семестре

«РАЗРАБОТКА МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СПЕЦИАЛИЗИРОВАННОГО ОБЪЕКТА»

Содержание:

1.	Введение	3
2.	Паспорт предприятия.	5
3.	Описание модели бизнес-процессов	9
4.	Задачи построения КСЗИ	10
5.	Этапы построения КСЗИ	11
6.	Расчет информационных рисков	13
7.	Разработка ПИБ	19
8.	Заключение	20
9.	Источники	21
10.	Приложения	

Введение

С каждым годом увеличивается количество информации, растет ее спрос, а значит и растет ее ценность, связи с этим возрастают требования по ее защите. Так же быстрыми темпами совершенствуются компьютерные технологии. Из-за ежегодного обновления компьютерных технологий возникают новые угрозы для информации. Следовательно, возрастет необходимость ее защиты. Для того чтобы защита была полной необходимо прорабатывать ее комплексно.

Утечка любой информации может отразиться на деятельности организации. Особую роль играет конфиденциальная информация, потеря корой может повлечь большие изменения в самой организации и материальные потери. Так как Администрация г. Воронежа является управленческим органом, то потеря конфиденциальной информации может повлечь потери не только для самой Администрации, как организации, так и для всего города в целом. Поэтому мероприятия по защите информации в данное время очень актуальны и важны.

Для обеспечения полноценной защиты конфиденциальной информации необходимо проводить комплексный анализ каналов утечки, каналов и методов несанкционированного воздействия на информацию.

Целью курсового проекта является разработка проекта КСЗИ на примере Администрации города Воронежа..

Задачи:

1.Проанализировать общую характеристику объекта защиты, оформленную в виде «Паспорта предприятия»;

2.Построить модель бизнес-процессов с целью выявления конфиденциальной информации;

3. Составить «Перечень сведений конфиденциального характера»;

4. Выявить объекты защиты, оформленные в виде «Списка объектов, подлежащих защите»;

5.Выявить угрозы, уязвимости и произвести расчет рисков для ключевых объектов защиты;

6.Построить модель злоумышленника;

7.Проанализировать степень защищенности объектов защиты по каждому из видов защиты информации (ЗИ) (правовая ЗИ, организационная ЗИ, программно-аппаратная ЗИ, инженерно-физическая ЗИ, криптографическая ЗИ);

Паспорт предприятия.

Здание Администрации находится в районе. По адресу г. Воронеж, ул. Ленина,1а. Здание Администрации является пятиэтажным. Имеет свой хозяйственный двор для служебного автотранспорта. Перед зданием имеется автопарковка. Вход людей в здание осуществляется через контрольно-пропускной пункт, находящемся на 1-ом этаже здания.

Доступ имеет свои разграничения:

— в Отдел, занимающийся вопросами работы с вопросами и просьбами населения, имеют доступ все посетители. Отдел находится на первом этаже здания.

— В отделы и помещения, находящиеся на втором этаже здания, где находиться конфиденциальная информация допуск осуществляемся только по пропускам.

— Во все остальные помещения и отделы имеют доступ лишь служащие и клиенты по записи,

— Доступ в кабинет Главы города в его отсутствие запрещен.

Границе КЗ Администрации является забор, ограничивающий периметр здания и хоз. двора..

Электропитание здания осуществляется от трансформаторной подстанции, которая расположена на неконтролируемой территории и обслуживается сторонней организацией.

Здание окружено жилыми домами (5- этажными).

В состав ВТСС входят:

— система кондиционирования (по одному в каждом кабинете);

— телефонный аппарат (в каждом кабинете, телефонная связь осуществляется через общую АТС здания, кабели АТС выходят за пределы КЗ) . В каждом отделе по 2.

— компьютер (на каждом рабочем месте, состав: системный блок, монитор, мышь, клавиатура, 2 динамика)

— принтер (в каждом отделе по 1 штуке).

— телевизор (1шт. в кабинете Главы города).

В Администрации в каждом кабинете по 1-3 окна, в зависимости от

площади кабинета. Все окна – тройной евростеклопакет. На окнах установлены жалюзи. Окна с одной стороны здания выходят на хоз. двор., остальные на шумные улицы

Количество стояков отопления соответствует количеству окон. Трубы системы отопления проходят по всем этажам, заканчиваются в бойлерной(подвальное помещение здания).

Стены, потолок – железобетонные плиты толщиной 400 мм, отделаны гипсокартонном толщиной10мм, пол – железобетонные плиты толщиной 400 мм, покрытые паркетом (отделы) и ковролином (кабинет Главы города).

Количество дверей соответствует количеству кабинетов в здании.

Дверь входа в здание – железная укрепленная.

Требования к монтажу кабельной проводки – скрытый монтаж.

Генераторы вибро-акустического зашумления не установлены.

Генераторы электромагнитного шума не установлены.

Направления деятельности Администрации:

— юридический отдел;

— комитет по управлению;

— отдел муниципального обслуживания;

— вопросами безопасности;

— проблемами строительства;

— вопросы ЗАГСа;

— вопросами коммунального хозяйства, распределения жилья;

— вопросы гуманитарного развития ;

— вопросы экономического развития;

— вопросами кадрового развития;

— вопросами хозяйственного обслуживания;

На предприятии отсутствуют сведения, составляющие государственную тайну, но ведется работа с коммерческой и служебной тайной. Существует ряд нормативно- правовых актов регламентирующих правила пользования этими сведениями.

В Администрации существует своя локальная сеть, доступ к которой имеют только служащие Администрации. В большинстве случаев имеется доступ лишь к ограниченному числу сайтов этой сети, необходимых в ходе трудовой деятельности. Информация о каждом выходе в сеть фиксируется системным администратором. Это также относится к сети Интернет.

Основными объектами защиты являются:

— АРМ сотрудников;

— сервер локальной сети;

— конфиденциальная информация (документы);

— кабинет Главы города;

— зал проведения совещаний;

— кабинеты с конфиденциальной документацией.

В Администрации разработана часть мер по защите информации:

— заключен договор об охране помещения и территории;

— разработан график работы и посещения населения;

— разработан режим и правила противопожарной безопасности;

— режим видеонаблюдения этажей;

— разработаны должностные инструкции служащих, разграничивающие их права и обязанности ;

—дополнительные соглашения к трудовым договорам сотрудников о неразглашении ими конфиденциальной информации, регламентирующие ответственность в области защиты информации;

— инструкции по охране периметра, по эксплуатации системы охранной сигнализации и видеонаблюдения;

— положение о конфиденциальном документообороте;

— описание технологического процесса обработки КИ;

— установлена антивирусная системы защиты на АРМ;

— разграничен доступ к АРМ паролями.

Описание модели бизнес-процессов.

Модель бизнес-процесса Администрации города Воронежа максимально подробно описан в Приложении №1, с помощью построения модели BPwin.

Проанализировав структуру Администрации можно выделить, что она имеет очень обширную сферу деятельности. Потому, что состоит из множества отделов. В каждом отделе рассматриваются различные вопросы по обеспечению жизнедеятельности города. Каждый отдел несет ответственность за свои действия.

Деятельность Администрации является очень важной, потому как это муниципальные орган управления города.

Задачи построения КСЗИ.

После анализа имеющихся данных можно выделить ряд задач необходимых для построения КСЗИ:

— дополнение имеющихся мер защиты, внедрение и организацию;

— составить комплекс организационных мероприятий;

—проработать перечень программно-аппаратных и инженерно-технических мер;

— необходимо составить перечень конфиденциальной информации;

— составляется перечень объектов защиты;

— определить перечень угроз для этих объектов;

— рассчитать информационные риски.

Рассмотрев состав информационных ресурсов предприятия, определяем состав конфиденциальной информации:

— Сведения, составляющие коммерческую тайну;

— Сведения, содержащие персональные данные.

Получаем перечень сведений, составляющих конфиденциальную информацию (Приложение №2);

Также необходимо определить местоположение защищаемой информации на предприятии. Для этого составляется перечень объектов защиты (Приложение №5), включающий структурную графическую схему второго этажа в здании Администрации (Приложение №6), где проходит основной поток конфиденциальной информации.

Этапы построения КСЗИ.

Для создания комплексной системы защиты информации на предприятии необходимо провести ряд мероприятий:

Эти мероприятия может проводить как специально приглашённая фирма-исполнитель, так и служба безопасности предприятия (если она имеет лицензию на осуществление этой деятельности).

1.Стартовый (начальный).

— Получение согласия высшего руководства на создание КСЗИ.

— Разработка плана работ по созданию КСЗИ.

— Формирование команды по созданию КСЗИ.

В результате проведения этого этапа должны появиться следующие документы:

— Приказ о создании КСЗИ,

— план работ по созданию КСЗИ,

— приказ о формировании команды,

— приказ о проведении обследования предприятия.

2. Этап предпроектного обследования.

На этом этапе проводится обследование (аудит) предприятия.

— Инвентаризация объектов информатизации и персонала.

— Выявление информационных потоков.

— Моделирование бизнес-процессов.

— Разработка отчёта, в который должны входить: объекты защиты с точки зрения угроз, модели злоумышленников, ответственные за объекты информатизации, расчёт рисков, ранжирование рисков.

— Разработка технического задания на проектирование КСЗИ. В него входят ключевые объекты защиты, меры и средства защиты, требования по защите.

3. Проектирование.

— Создание системного проекта.

— Создание “Политики безопасности”.

— Проведение работ по созданию КСЗИ (технический проект с опорой на ресурсы, «Технический проект на создание КСЗИ» представляет собой комплект документов, в который входит часть документов разработанных на предыдущих этапах и ряд новых документов, в которых описано, как именно будет создаваться, эксплуатироваться и, в случае необходимости, модернизироваться КСЗИ).

— Создание рабочего проекта.

4. Внедрение

На этом этапе создаётся пакет документов «Эксплуатационная документация на КСЗИ», который включает:

— Инструкции эксплуатации КСЗИ и её элементов;

— Процедуры регламентного обслуживания КСЗИ;

— Правила и положения по проведению тестирования и анализа работы КСЗИ.

На этом этапе проводится все пусконаладочные работы, обучает и инструктирует персонал предприятия правилам и режимам эксплуатации КСЗИ.

После реализации этого этапа внедренная КСЗИ готова к последующему испытанию. В процессе испытаний выполняются тестовые задания и контролируются полученные результаты, которые и являются индикатором работоспособности спроектированной КСЗИ. По результату испытания КСЗИ делается вывод относительно возможности представления КСЗИ на государственную экспертизу.

Расчет информационных рисков.

Критичность ресурса (D) – степень значимости ресурса. Отражает влияние реализации угрозы на работу информационной системы.

Критичность реализации угрозы (ER) – степень влияния реализации угрозы на ресурс. Задается в %.

Вероятность реализации угрозы через данную уязвимость в течении года (P(v)) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях, указывается в %.

1. Объект защиты – автоматизированное рабочее место **(АРМ) сотрудника.**

Критерий критичности (D) равен 5000 рублей.

Таблица угроз и уязвимостей.

Угроза	*Уязвимости*
1.Физический доступ нарушителя к АРМ	1. Отсутствие системы контроля доступа служащих к чужим АРМам
	2.Отсутствие системы видеонаблюдения на предприятии
	3. Несогласованность в системе охраны периметра задания
2.Разглашение КИ, хранящейся на АРМ	1.Отсутствие соглашения о неразглашении между Администрацией и служащими.
	2.Нечеткое распределение ответственности между служащими
3.Разрушение КИ при помощи специальных программ и вирусов	1.Отсутствие или некорректная работа антивирусного ПО
	2.Отсутствие ограничения доступа пользователей к внешней сети

Таблица вероятности реализации данной угрозы через уязвимость в течении года(P(V)) и критичности реализации угрозы (ER).

Угроза/уязвимость	*P(V), %*	*ER,%*
1/1	50	50
1/2	30	50
1/3	10	40
2/1	30	40
2/2	50	40
3/1	10	90
3/2	20	60

Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

Угроза/уязвимость	*Th*	*CTh*
1/1	0,25	0,975
1/2	0,15	
1/3	0,04	
2/1	0,12	0,296
2/2	0,2	
3/1	0,09	0,199
3/2	0,12	

Th=P(V)/100*ER/100
CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:
CThR=1-П(1-CTh)=1-0,025*0,04*0,801=0,986
Рассчитаем риск по ресурсу:
R= CThR*D=0,986*7500=**7395 (руб).**
Объект защиты – **сервер локальной сети.**
Критерий критичности (D) равен 15000 рублей.

Таблица угроз и уязвимостей.

Угроза	*Уязвимости*
1.Физический доступ нарушителя к серверу	1.Неорганизованность контрольно-пропускного режима на предприятии
	2.Отсутствие видеонаблюдения
2.Разглашение КИ, хранящейся на сервере	1.Отсутствие соглашения о нераспространении КИ
	2. Нечеткое распределение ответственности между сотрудниками предприятия

Таблица вероятности реализации данной угрозы через уязвимость в течении года(P(V) и критичности реализации угрозы (ER).

Угроза/уязвимость	*P(V), %*	*ER,%*
1/1	70	80
1/2	40	60
2/1	30	30
2/2	70	50

Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

Угроза/уязвимость	*Th*	*CTh*
1/1	0,56	0,666
1/2	0,24	
2/1	0,09	0,408
2/2	0,35	

Th=P(V)/100*ER/100
CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:
CThR=1-П(1-CTh)=1-0,344*0,592=0,796
Рассчитаем риск по ресурсу:
R=CTh*D=0,796*15000=**11940 (руб).**

2. Объект защиты – **Конфиденциальная документация.**
Критерий критичности (D) равен 3000 рублей.

Таблица угроз и уязвимостей.

Угроза	*Уязвимости*
1.Физический доступ нарушителя к документам	1.Неорганизованность контрольно-пропускного режима на предприятии
	2.Отсутствие видеонаблюдения
2.Разглашение КИ, используемой в документах, вынос документов за пределы КЗ	1.Отсутствие соглашения о неразглашении КИ
	2. Нечеткое распределение ответственности за документы между сотрудниками предприятия
3.Несанкционированное копирование, печать и размножение КД	1. Нечеткая организация конфиденциального документооборота
	2. Неконтролируемый доступ сотрудников к копировальной и множительной технике

Таблица вероятности реализации данной угрозы через уязвимость в течении года(P(V) и критичности реализации угрозы (ER).

Угроза/уязвимость	*P(V), %*	*ER,%*
1/1	70	80
1/2	40	60
2/1	30	30
2/2	70	50
3/1	70	50
3/2	90	80

Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

Угроза/уязвимость	*Th*	*CTh*
1/1	0,56	0,666
1/2	0,24	
2/1	0,09	0,408
2/2	0,35	
3/1	0,35	0,818
3/2	0,72	

Th=P(V)/100*ER/100
CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:
CThR=1-П(1-CTh)=1-0,334*0,592*0,182=0,964
Рассчитаем риск по ресурсу:
R=CTh*D=0,964*3000=**2892 (руб).**

Администрация города Воронежа является государственной организацией, поэтому деньги на создание комплексной системы защиты информации будут выделяться из городского бюджета.

Из оценки рисков можно подсчитать какой ущерб может понести Администрация при реализации той. Так же мы можем оценить экономическую целесообразность построения КСЗИ.

Если потери при реализации информационных угроз являются незначительными, то не имеет смысла строить дорогостоящую КСЗИ.

Еще одним важным шагом является разработка Технического задания на КСЗИ (Приложение №3).Оно определяет все основные требования к КСЗИ и возможные пути реализации её составляющих элементов. В ТЗ формулируются и исследуются основные каналы утечки информации и пути и средства их локализации.

Разработка политики безопасности.

Под политикой информационной безопасности (ИБ) понимается совокупность документированных управленческих решений, направленных на защиту информационных ресурсов организации. Это позволяет обеспечить эффективное управление и поддержку политики в области информационной безопасности со стороны руководства организации.

Политика ИБ является объектом стандартизации. Некоторые страны имеют национальные стандарты, определяющие основное содержание подобных документов. Имеются ряд ведомственных стандартов и международные стандарты в этой области (ISO 17799).

В России к нормативным документам, определяющим содержание политики ИБ, относится ряд РД ФСТЭКа. В отечественных и международные стандартах используются сходная методология, однако ряд вопросов в отечественных РД не рассмотрен или рассмотрен менее подробно. Таким образом, при разработке политики ИБ целесообразно использовать передовые зарубежные стандарты, позволяющие разработать более качественные документы, полностью соответствующие отечественным РД.

Целью разработки политики организации в области информационной безопасности является определение правильного (с точки зрения организации) способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности.

Основные этапы:

Разработка концепции политики информационной безопасности

Описание границ системы и построение модели ИС с позиции безопасности

Анализ рисков: формализация системы приоритетов организации в области информационной безопасности, выявление существующих рисков и оценка их параметров

Анализ возможных вариантов контрмер и оценка их эффективности.

Выбор комплексной системы защиты на всех этапах жизненного цикла

Заключение.

Таким образом, поставив перед собой цель разработать проект КСЗИ в Администрации города Воронежа, мною были проделаны следующие работы:

1.Я рассмотрела общую характеристику объекта защиты;

2.Построила модель бизнес-процессов с целью выявления конфиденциальной информации;

3. Составила «Перечень сведений конфиденциального характера»;

4.Выявила угрозы, уязвимости и произвела расчет рисков для ключевых объектов защиты;

5.Описала техническое задание

6.Рассмотрела политику безопасности.

7.Получить теоретические знания и практические навыки в создание эффективной системы защиты информации.

Я считаю, что построение КСЗИ в таком муниципальном органе, как городская Администрация необходима.

«Техническое задание на систему защиты информации»

приложение 1
к Договору №_____от
«____»_____2005г.

Для внутреннего пользования
Экз. №__

От Заказчика:	От Исполнителя:
Первый заместитель главы города	Генеральный директор ОАО «Безопасность»
_____ ФИО	_____ ФИО
«___» _____ 2014 г.	«___» _____ 2014 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание КСЗИ Администрации города Воронежа

Термины и определения

ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ (ДСП) – конфиденциальная информация, которая: либо получена в процессе производственной деятельности от государственных предприятий и организаций, либо создана для государственных организаций при обработке информации, полученной от любых контрагентов. Либо изначальным, либо конечным собственником данной информации ограниченного распространения является государство. От утечки данной информации могут пострадать интересы государства.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПД) - конфиденциальная информация о частной жизни физического лица, которая получена в процессе

производственной деятельности от любых контрагентов. Собственником данной информации ограниченного распространения является физическое лицо. От утечки данной информации могут пострадать интересы этого физического лица.

НЕ СЕКРЕТНО (НС) – открытая информация, доступ к которой не ограничивается требованиями безопасности либо согласно производственной необходимости (общий доступ и т.п.), либо как не подлежащая засекречиванию в соответствии с законодательством (данные бухгалтерского учета и т.п.)

КОНТРОЛИРУЕМАЯ ЗОНА (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей КЗ Организации является: периметр охраняемой территории Организации; ограждающие конструкции охраняемого здания или охраняемой части здания.

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. К ним относятся средства вычислительной техники, средства и системы передачи данных, отображения и размножения документов.

ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС. К ним относятся: радио- и телефонные средства и системы; средства и системы охранной и пожарной сигнализации; контрольно-измерительная аппаратура; средства и системы кондиционирования; средства и системы проводной радиотрансляционной и телевизионной сети; средства электронной оргтехники; средства вычислительной техники, не предназначенные для передачи, обработки и хранения конфиденциальной информации.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) – нарушение установленных правил доступа (организационных, технических и программных ограничений) к конфиденциальной информации, преднамеренное либо не преднамеренное, независимо от результата (получен фактический доступ к этой информации или нет).

ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ (ПЭМИН) – распространение электромагнитного излучения, возникающего в результате обработки конфиденциальной информации, в окружающем пространстве (по эфиру), а также по металлическим проводникам (коммуникациям), и позволяющего интерпретировать данную информацию.

КОНФИДЕНЦИАЛЬНАЯ ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ (ЛВС) – комплекс средств вычислительной техники, соединенных каналами передачи данных, не выходящими за пределы КЗ, и предназначенных для обработки конфиденциальной информации. ЛВС функционально может являться частью вычислительной сети Организации (в остальных частях

обрабатывается не конфиденциальная информация), а организационно – это часть АС, расположенная в пределах КЗ.

Общая характеристика объекта.

Предметом защиты является конфиденциальная информация в Администрации города Воронежа. Эта информация циркулирует в определенных подразделениях, а также в электронном виде располагается на сервере корпоративной сети.

В этом органе государственно управления конфиденциальная информация создается, обрабатывается, используется и уничтожается.

Выделяют сведения конфиденциального характера на основании следующих документов:

Сведениям различной степени конфиденциальности в соответствии с СТР-К собственниками информации должны присваиваться соответствующие грифы конфиденциальности. На основании анализа входящих документов выявлено следующее:

Конфиденциальная информация в подразделениях Администрации обрабатывается с помощью офисных приложений, ведомственного прикладного программного обеспечения (ПО) с использованием систем управления базами данных (СУБД) и служебных утилит.

Границей КЗ Администрации является ограждающая конструкция территории. Особенностью КЗ является присутствие на контролируемой территории посторонних лиц (ведется прием посетителей).

Телефонная связь в Администрации осуществляется через общую АТС и внутреннюю. Кабели общей АТС выходят за пределы КЗ.

Пожарная и охранная сигнализации установлены во всех помещениях здания.

Электропитание всего здания осуществляется от трансформаторной подстанции, которая расположена на контролируемой территории и обслуживается персоналом станции.

Доступ к информации.

Доступ на территорию Администрации осуществляется свободно, кроме второго этаже где находится КПП. Пропускной режим обеспечивается круглосуточно силами сотрудников вневедомственной охраны УВД. Доступ на территорию Администрации и в помещения, где хранится кон информация, осуществляется по служебному удостоверению либо по специальной отметке в пропуске.

Допуск служащих Администрации к защищаемым информационным ресурсам осуществляется в соответствии с должностными обязанностями, утвержденными службой безопасности, и разграничивается штатными средствами ОС. Физический доступ к серверу и активному сетевому

оборудованию ограничен, они размещены на втором этаже здания, в отдельном кабинете, в закрывающихся телекоммуникационных шкафах.

Для передачи данных между пользователями АРМ используются автоматизированные системы документооборота (внутренняя электронная почта, средства передачи сообщений).

Информационная характеристика.

В технологическом процессе обработки конфиденциальной информации определены следующие компоненты:

- субъекты доступа;
- объекты доступа.

К субъектам доступа относятся:

- служащие, имеющие отношение к процессу функционирования Администрации и которые имеют возможность доступа к её ресурсам;
- процедуры (процессы) обработки данных прикладного и системного ПО, а также СУБД, которые получают данные из файлов и баз данных на сервере.

К объектам доступа относятся:

- информационные ресурсы – отдельные файлы и массивы файлов, поля, записи и таблицы БД, документы, машинные носители информации (НЖМД, НГМД, CD-RW (CD-R) диски), доступ к которым должен регламентироваться правилами разграничения доступа;
- элементы системы – средства обработки и передачи информации (технические и программные средства, средства приема, отображения, перемещения информации, машинные накопители и носители на бумажной основе), доступ к которым необходимо регламентировать.

На ПЭВМ пользователей и на сервере установлены операционные системы семейства Microsoft Windows (XP), но система управления пользователями и разграничения доступа к файловым ресурсам не является централизованной (доменная структура отсутствует).

Каналы утечки информации.

К возможным каналам утечки или нарушения целостности информации можно отнести:

- НСД к информации, обрабатываемой на ПЭВМ и на сервере;
- НСД к бумажным и машинным носителям информации;
- выход из строя технических и программных средств, в т.ч. машинных носителей информации.

Нарушение целостности информации возможно как путем физического разрушения носителей информации, так и путем искажения ее с помощью программных средств:

- Аварии, стихийные бедствия (пожар, затопление);

- Колебания в сети электропитания;
- Старение магнитной поверхности носителей информации;
- Ошибочное удаление информации пользователем;
- Сбои прикладного программного обеспечения.

Возможны следующие способы несанкционированного доступа к защищаемым ресурсам АС:

- физический доступ к носителям информации (к серверу) и их резервным копиям с целью их хищения;
- физический доступ к бумажным носителям информации, с целью их хищения, размножения, фотографирования;
- непосредственный (вне рамок прикладного ПО) доступ к файлам хранилища информации, таблицам БД и исполняемым модулям ПО - удаленно или локально с целью их копирования и дальнейшей установки, а также с целью их уничтожения;
- применение нештатных специальных программ, обеспечивающих восстановление удаленных данных с машинных носителей информации;
- передача файлов по каналам связи между сотрудниками и за пределы станции с целью предоставления НСД лицам, не имеющим допуска к данной информации в обход штатных средств защиты;
- доступ в рамках прикладного ПО локально или удаленно к базам данных и файлам с использованием недокументированных возможностей и режимов работы этого ПО, разработанных и установленных в качестве модификаций, в случае, когда разработчиком ПО является сторонняя организация;
- любой доступ к ПО и данным с использованием технологий взлома средств защиты с целью получения или уничтожения данных (в т.ч. компьютерные вирусы);
- доступ с использованием чужого идентификатора, а также с чужого рабочего места во время отсутствия пользователя этого АРМ.

Модель нарушителя

В качестве возможного нарушителя рассматривается субъект, имеющий доступ к работе с программными и техническими средствами. Нарушители классифицируются по уровню возможностей, предоставляемых им всеми доступными средствами (Таблица 1).

Таблица 1.

Уро-вень	Возможности нарушителя по технологическому процессу	Потенциальная группа нарушителей	Возможный результат НСД
1	Нет	Служащие, не имеющие доступа к информации, но имеющие доступ в помещения (обслуживающий персонал, посетители)	Просмотр на экране монитора и хищение бумажных и машинных носителей.

2	Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации	Большинство пользователей АС, имеющих непосредственный доступ в помещения, к АРМ, с полномочиями, ограниченными на уровне системы защиты информации (СЗИ)	Доступ пользователя к информации другого пользователя в его отсутствие, в т.ч. через сеть, просмотр информации на мониторе (несоблюдение организационных требований). Просмотр и хищение бумажных носителей.
3	Управление функционированием АС, т.е. воздействие на базовое программное обеспечение ОС и СУБД, на состав и конфигурацию оборудования АС, на настройки СЗИ. Работа с внешними носителями.	Администраторы АС, наделенные неограниченными полномочиями по управлению ресурсами	Доступ администратора АС к информации других пользователей и к средствам СЗИ, непреднамеренное разрушение информации (несоблюдение организационных требований)
4	Весь объем ностей лиц, твляющих ремонт еских средств АС.	Обслуживающий персонал АС. листы сторонних организаций, твляющих поставку и монтаж ования для АС	Доступ обслуживающего ала АС к МН с мацией других вателей, разрушение мации, установка закладных ств (несоблюдение зационных требований при е ОТСС)

Фактическая защищенность

Доступ служащих к ресурсам разграничивается штатными средствами ОС. Список служащих, имеющих доступ к ресурсам, документально определен. Доступ ограничивается в соответствии с должностными инструкциями.

Документ, определяющий порядок конфиденциального документооборота существует и утвержден.

Документально определена технология обработки информации (документ «Описание технологического процесса обработки информации»).

На серверах и рабочих станциях применяются операционные системы MS Windows, что позволяет применить сертифицированные средства защиты от НСД. Но также осуществляется обработка информации в СУБД, что практически исключает применение на данных объектах сертифицированных средств защиты от НСД по причине отсутствия таких средств на рынке.

Перечень мер по защите

Разработка перечня защищаемой информации

- Необходимо переработать перечень сведений конфиденциального характера в плане детализации обрабатываемых данных и отнесении сведений к той или иной степени конфиденциальности.

Конфиденциальность информации

С целью повышения степени защищенности информации в плане соблюдения конфиденциальности необходимо:

- разделить ввод и вывод информации одного грифа на уровне АРМ или пользователей с целью разделения ответственности и усиления контроля за этими этапами технологического процесса;
- ограничить (в т.ч. организационно) возможности несанкционированного вывода информации пользователями на внешние носители (дискеты, лазерные накопители CD-RW, USB-Flash) и на печать;
- ограничить количество или исключить использование локальных принтеров на АРМ пользователей, назначить ответственных за печать документов на сетевых принтерах;
- исключить доступ пользователей к ресурсам АРМ других пользователей, как на запись, так и на чтение, т.е. возможность создания пользователями общих сетевых ресурсов на своих АРМ. Обмен информацией между пользователями осуществлять через общие ресурсы на серверах;
- если один служащий относится к нескольким категориям пользователей, то при совмещении обязанностей он должен пользоваться разными идентификаторами. Например, администратор может выполнять работу пользователя, но не имеет права делать это с идентификатором администратора.

Целостность информации

С целью повышения степени защищенности информации в плане соблюдения целостности необходимо:

- внедрение исправлений и добавлений централизованно распространяемых ведомственных программных средств на АРМ пользователей и на сервер должно осуществляться в виде уже откомпилированных исполняемых модулей и процедур, в состав которых не должны включаться средства отладки.

Состав рабочей документации

Для документального определения режимов обработки и защиты информации в состав рабочей (исполнительной) документации по защите конфиденциальной информации необходимо включить следующие документы:

- «Описание технологического процесса обработки конфиденциальной информации», в котором отражен порядок проведения всех операций ТП (ввод, вывод, обработка и хранение, резервирование и восстановление, управление доступом);
- «Инструкция пользователя», в которой отражены порядок его работы с информацией, права, обязанности и ответственность;
- «Инструкции администраторов ОС, БД»;
- «Инструкция обслуживающего персонала»;

- «Журнал регистрации бумажных носителей информации», в котором учитываются все операции распечатывания документов, графы журнала заполняются исполнителями работ;
- «Журнал учета резервного копирования», в котором учитываются все операции резервного копирования и восстановления информации, все графы журнала заполняют администраторы.
- Перечень сведение конфиденциального характера Администрации города Воронежа.

I. Общие положения.

1. Назначение документа.

Политика является основой для:

1. Разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности информации;

2. Принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

3. Координации деятельности структурных подразделений Администрации при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований обеспечения безопасности информации.

2. Основания для разработки документа.

1. Приказ главы Администрации города Воронежа о создании Политики Информационной Безопасности Администрации.

2. Законодательной базой ПИБ являются: Конституция РФ, Гражданский и Уголовный кодексы, нормативные документы действующего законодательства, документы Федеральной службы технического и экспертного контроля, организационно- распорядительные документы Администрации.

3. Основные определения и сокращения.

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Разглашение КИ – несанкционированный выход защищаемых сведений и документов за пределы круга лиц, которым они доверены или стали известны в ходе их трудовой деятельности.

Разрешительная (разграничительная) система доступа к информации – совокупность обязательных норм, устанавливаемых первым руководителем или коллективным органом руководства фирмой с целью закрепления за руководителями и сотрудниками права использования для выполнения

служебных обязанностей выделенных помещений, рабочих мест, определенного состава документов и ценных сведений.

Сервер – аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей ввиду высоких требований по обеспечению надёжности, степени готовности и мер безопасности ИС предприятия.

Автоматизированная станция - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Коммерческая тайна – это конфиденциальная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны (то есть, приняты меры по охране её конфиденциальности).

Информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Нарушитель – это лицо, которое предприняло попытку выполнения запрещённых операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные методы, возможности и средства.

АРМ – автоматизированное рабочее место
АС – автоматизированная станция
ЗИ – защита информации
ИБ – информационная безопасность
ИТ – информационные технологии
КД – конфиденциальные документы
КИ – конфиденциальная информация
КТ – коммерческая тайна
ЛВС – локальная вычислительная сеть
НДВ – не декларированные возможности
НСД – несанкционированный доступ
ПБ – политика безопасности
ПИ – персональный идентификатор
ПК – персональный компьютер
ПО – программное обеспечение
ПЭВМ – персональная электронно-вычислительная машина
ПЭМИН – побочные электромагнитные излучения и наводки
ОС – операционная система
ЧС – чрезвычайная ситуация
ЭЛТ – электронно-лучевая трубка

II. Описание информационной системы.

1. Ответственность подразделений.

Ответственность подразделений распределяется следующим образом:

– За поддержание ИС в рабочем состоянии и обеспечение её функционирования ответственно Системный администратор;

– За физическую сохранность оборудование и носителей информации ответственна Служба безопасности;

– За информационную безопасность и обеспечение конфиденциальности информации ответственен специалист по защите информации.

2. Режим функционирования системы.

Режим функционирования информационной системы – только в рабочее время. В целях выполнения регламентных работ по обслуживанию оборудования или программного обеспечения системы возможна остановка в работе отдельных элементов системы (сервера.) без ущерба для общей функциональности.

При возникновении сбоев соответствующее сообщение сохраняется подсистемой журнал копирования в системном журнале.

3. Цели и задачи политики безопасности.

Цель: обеспечение защиты информации от ее искажения, модификации, утраты, которые могут привести к нарушению работы администрации, как муниципального органа управления.

Задачи политики безопасности:

- выявление действующих и потенциальных угроз;
- разработка методов противодействия выявленным угрозам;

определение оптимального количества сил и средств, необходимых для обеспечения безопасности.

III. Средства управления.

1. Оценка рисков и управление ими.
2. Экспертиза системы ЗИ (существующие средства ЗИ).
3. Правила поведения, должностные обязанности и ответственность.
4. Планирование безопасности.
5. Разрешение на ввод компонентов в строй (любого компонента ИС и системы ЗИ).
6. Порядок подключения подсетей подразделений к сетям общего пользования.

IV. Функциональные средства.

1. Защита персонала.
2. Управление работой и вводом/выводом информации.
3. Планирование непрерывной работы.
4. Средства поддержки программных приложений.

Для поддержки программных приложений, системный администратор обязательном порядке, каждое утро проверяет наличие обновлений на сайтах

производителей установленного ПО и, при наличии, принимает меры по исправлению сложившейся ситуации.

5. Средства обеспечения целостности информации.

В случае обнаружения несовпадения контрольных сумм – осуществляется восстановление данных из резервных копий.

Резервные копии информации и программного обеспечения должны извлекаться и тестироваться на регулярной основе.

6. Документирование (вся структура документов по ИС и СЗИ + правила составления документов).

Документация должна включать записи решений руководства для обеспечения отслеживаемости действий к решениям руководства и политикам, а также воспроизводимости записанных результатов.

В структуру документации по системе защиты информации входят:

- Перечень сведений конфиденциального характера;
- Перечень персональных данных;
- Положение о конфиденциальном документообороте;
- Техническое задание на проведение работ по созданию комплексной системы защиты информации;
- Технологический процесс обработки информации в информационной системе;
- Технический паспорт информационной системы;
- Перечень угроз информационной системы;
- Печень объектов защиты.

Разрабатываемая документация оформляется в соответствии с ГОСТ РД 50-34.698-90 и ГОСТ 6.10-84, а так же «Положением о конфиденциальном документообороте».

7. Осведомлённость и обучение специалистов.

В целях оперативного оповещения о произошедших инцидентах, плановых и внеплановых работ, ограничении функциональности и изменениях в документах, посвященных системе защиты информации оповещаются все служащие посредствам совещаний..

Все служащие Администрации должны в обязательном порядке проходить обучение по вопросам информационной безопасности. Для персонала непосредственно участвующего в процессе разработки или поддержки функционирования информационной системы и системы безопасности такое обучение должно проходить не реже 1 раза в год, для всего остального персонала – не реже 1 раза в 3 года, для вновь принятых на работу – перед вступлением в должность.

8. Ответные действия, в случае возникновения происшествий.

Все инциденты информационной безопасности должны записываться в базу знаний для дальнейшего анализа и выработки решений для предотвращения подобных происшествий в будущем.

Кроме того должны быть разработаны и утверждены инструкции по действиям в аварийных ситуациях (пожар, затопление и др.).

V. Технические средства.

1. Требования к процедурам идентификации и аутентификации.

Процедуры идентификации и аутентификации должны обеспечивать надёжный контроль доступа к ресурсам ИС.

2. Требования к системам контроля разграничения доступа.

Система контроля доступа должна обеспечивать надёжный контроль доступа к ресурсам ИС.

3. Требования к системе регистрации событий в ИС.

Система регистрации должна обеспечивать запись всех событий, происходящих в ИС, а так же предоставлять данные записи в удобочитаемом виде, для последующего ознакомления с ними соответствующими сотрудниками.

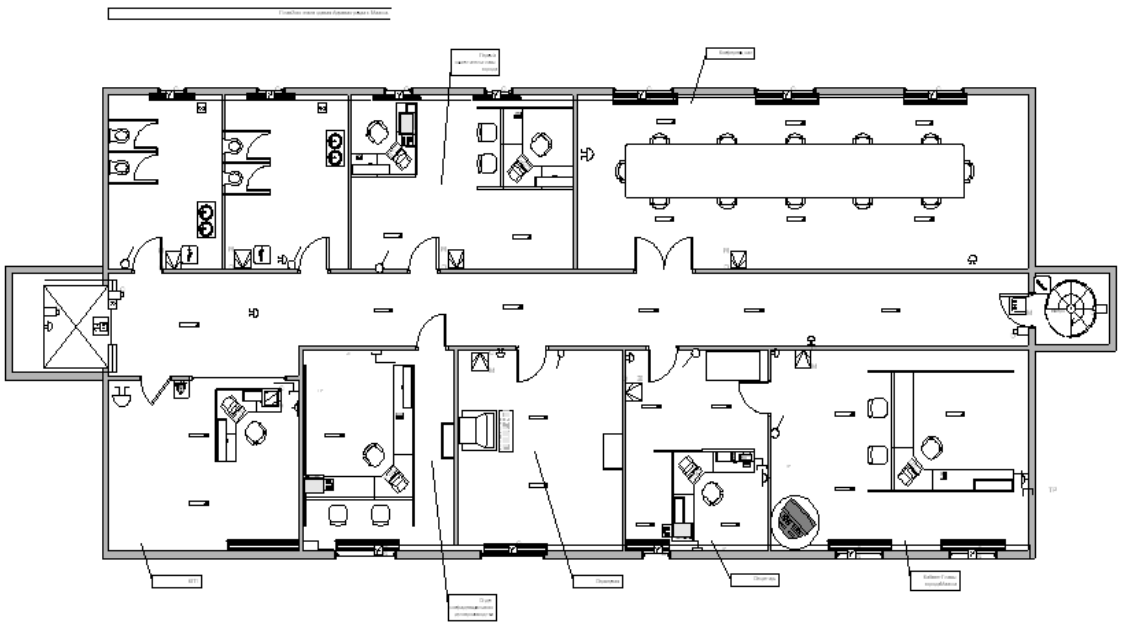
ПРИЛОЖЕНИЕ №5

1. Автоматизированные системы различного уровня и назначения

1.1. Автоматизированные рабочие места служащих

1.2. АРМ секретаря главы города

1.3. АРМ главы города



2. Системы связи, системы отображения и размножения

2.1. средства и системы телефонной, внутренней телефонной, громкоговорящей связи;

2.2. телефонная система «Внутренняя»

2.3. средства и системы звукоусиления;

2.4. система конфиденциального делопроизводства (учет, размножение и движение бумажных и прочих внешних носителей информации);

2.5. система обработки информации в вычислительной сети (ввод, вычисления, хранение, вывод);

2.6. система обработки речевой информации в специально предназначенных (защищаемых) помещениях (переговоры, совещания);

2.7. автоматизированная система передачи информации между сетями по неконтролируемой территории (файлы, базы данных, факсы, телефонные разговоры).

Примерные темы курсовых проектов

1. Разработка мероприятий по защите информации для системы управления ООО « Воронежсельмаш».
2. Разработка мероприятий по защите информации для системы управления ЗАО «Рудгормаш».
3. Разработка мероприятий по защите информации для системы управления ЗАО ВКСМ.
4. Разработка мероприятий по защите информации для системы управления ООО завод им. Тельмана.
5. Разработка мероприятий по защите информации для системы управления ОАО Электроприбор.
6. Разработка мероприятий по защите информации для системы управления ООО Финист-мыловар.
7. Разработка мероприятий по защите информации для системы управления ООО Ангстрем.
8. Разработка мероприятий по защите информации для системы управления ООО ВЭКС.
9. Разработка мероприятий по защите информации для системы управления ООО Воронежский шинный завод.
10. Разработка мероприятий по защите информации для системы управления ООО Воронежский станкостроительный завод.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО И ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ЗНАНИЙ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

№ п/п	Компетенция (общекультурная – ОК; профессиональная – ПК)	Форма контроля	семестр
1	(ОК-3) готовностью к активному общению с коллегами в научной, производственной и социально-общественной сферах деятельности	Тестирование (Т) Курсовой проект (КП) Зачет	3
2	(ОПК-4) способностью самостоятельно приобретать и использовать в практической деятельности новые знания и умения в своей предметной области	Тестирование (Т) Курсовой проект (КП) Зачет	3
3	(ПК-10) способностью использовать современные технологии	Тестирование (Т) Курсовой проект (КП)	3

	обработки информации, современные технические средства управления, вычислительную технику, технологии компьютерных сетей и телекоммуникаций при проектировании систем автоматизации и управления	Зачет	
4	(ПК-13) способностью разрабатывать и применять современные технологии создания программных комплексов и	Тестирование (Т) Курсовой проект (КП) Зачет	3
5	(ПК-18) готовностью участвовать в поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции.	Тестирование (Т) Курсовой проект (КП) Зачет	3

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Дескриптор компетенции	**Показатель оценивания**	**Форма контроля**				
		КП	**КР**	**Т**	**Зачет**	**Экзамен**
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	+		+	+	
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	+		+	+	
Владеет	программными продуктами для защиты информации в в	+		+	+	

	интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)					

7.2.1.Этап текущего контроля знаний

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по пятибальной шкале с оценками:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно».

Дескриптор компетенции	**Показатель оценивания**	**Оценка**	**Критерий оценивания**
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	отлично	Полное или частичное посещение лекционных, лабораторных и практических занятий. Выполненные КР, КрР на оценки «отлично».
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	хорошо	Полное или частичное посещение лекционных, лабораторных и практических занятий. Выполненные КР, Кр на оценки «хорошо».
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	удовлетворительно	Полное или частичное посещение лекционных, лабораторных и практических занятий. Выполненные КР, Кр.
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности,		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	неудовлетворительно	Частичное посещение лекционных, лабораторных и практических занятий. Частично выполненные КР, Кр.
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	не аттестован	Непосещение лекционных, лабораторных и практических занятий. Невыполненные КР, Кр
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		

7.2.2. Этап промежуточного контроля знаний

В третьем семестре результаты промежуточного контроля знаний (зачет) оцениваются по четырехбальной шкале с оценками:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «не удовлетворительно».

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	отлично	Студент демонстрирует полное понимание заданий. Все требования, предъявляемые к заданию выполнены.
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	хорошо	Студент демонстрирует значительное понимание заданий. Все требования, предъявляемые к заданию выполнены.
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	удовлетворительно	Студент демонстрирует частичное понимание заданий. Большинство требований, предъявляемых к заданию выполнены.
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления,		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Знает	фундаментальные основы защиты информации в интегрированных технических системах управления, критерии и классы защищенности информации, виды информационных угроз, технологии защиты корпоративных ИСУ и перспективы развития ИСУ (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)	неудовлетворительно	1. Студент демонстрирует небольшое понимание заданий. Многие требования, предъявляемые к заданию не выполнены. 2. Студент демонстрирует непонимание заданий. 3. У студента нет ответа. Не было попытки выполнить задание.
Умеет	самостоятельно разрабатывать модули защиты информации в интегрированных технических системах управления, обеспечивать элементарные мероприятия по защите информации (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		
Владеет	программными продуктами для защиты информации в в интегрированных технических системах управления, средствами оценки защищенности, средствами поддержании единого информационного пространства планирования и управления предприятием на всех этапах жизненного цикла производимой продукции (ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18)		

7.3. Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

Текущий контроль успеваемости осуществляется на практических занятиях: в виде опроса теоретического материла и умения применять его к решению задач у доски, в виде проверки домашних заданий, в виде тестирования по отдельным темам.

Промежуточный контроль осуществляется проведением контрольных работ по отдельным разделам дисциплины, тестирования по разделам дисциплины, изученным студентом в период между аттестациями, проведением коллоквиумов по теоретическому материалу, выполнением расчетно-графических работ. Контрольные работы проводятся на практических занятиях

в рамках самостоятельной работы под контролем преподавателя. Варианты расчетно - графических работ выдаются каждому студенту индивидуально.

7.3.2. Примерная тематика и содержание КР

3-й семестр

ТЕСТ

Укажите основные свойства VPN

Создает туннель, т.е. защищённый канал передачи данных
Использует шифрование данных
Реализуется в незащищенных или слабо защищенных сетях

Каковы функциональные возможности программы Retina WiFi Scanner

Вычисляет WEP-ключи методом brute force
Генерирует отчёты
Обнаруживает IP-адреса и другую сетевую информацию
Обнаруживает неавторизованные беспроводные устройства

64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности

Высокий

Отметьте потенциально опасные с точки зрения утечек внутренней информации действия

Размещение серверов в стороннем дата-центре
Хранение носителей вне офиса
Сервисный ремонт серверов или жестких дисков
Перевозка компьютеров или носителей

Перебор всех слов языка для взлома пароля это

атака Brute Force

Какого типа БД является реестр

иерархическая

IDS - это

система обнаружения вторжений

Какие режимы работы имеет программа Iris

Decode
Capture

Используется ли VPN для защиты беспроводных сетей

да

Какие дополнительные меры обеспечения безопасности могут использоваться в беспроводных сетях

Технология VPN
Использование IPSec для защиты трафика
Защита беспроводного сегмента с помощью L2TP
Выделение беспроводной сети в отдельный сегмент

Инсайдер - это

член какой-либо группы людей, имеющий доступ к секретной, скрытой или какой-либо другой закрытой информации или знаниями, недоступной широкой публике

Сколько root key содержит реестр Windows

5

Решение DeviceLock является

программно-аппаратным

Способ построения одноранговых Wi-Fi сетей называется

Ad-hoc

Какие решения применяются для контроля доступа к внешним устройствам

Secret Disk
ZLock
DeviceLock

Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн слов

0,1 секунды

Сколько групп символов должен минимально содержать надежный пароль

3

Тонкий клиент - это

Бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер

В какой блок файла autorun.inf обычно прописываются вредоносные программы

open

Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет

500

Какой протокол VPN используется для создания защищенного сегмента локальной сети

IpSec

DLP (Data Leak Prevention) система защищает от

утечек конфиденциальной информации из информационной системы вовне

Что позволяет выполнять программа Process Monitor

Отслеживать сетевую активность процесса
Отслеживать обращение процесса к реестру
Отслеживать работу процесса с файлами

Необходимы ли криптографические ключи для создания VPN-тоннеля

Да

1 **Каковы предпосылки возникновения искусственного интеллекта как науки?**

-появление ЭВМ
-развитие кибернетики, математики, философии, психологии и т.д.
-научная фантастика
-нет правильного ответа

2 **В каком году появился термин искусственный интеллект (artificial intelligence)?**

-1856
-1956
-1954
-1950
-Нет правильного ответа

3 **Кто считается родоначальником искусственного интеллекта**?

-А. Тьюринг
-Аристотель
-Р. Луллий
-Декарт
-правильного ответа

Вопросы для самостоятельной проработки

1. Определить место информационной безопасности в обеспечении

системы общественной безопасности.

2. Дать определение информационной безопасности.

3. Назвать основные направления и задачи обеспечения информационной безопасности общества.

4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.

5. Охарактеризовать уровни реализации информационной безопасности.

6. Дать определение и классификацию информационных ресурсов.

7. Определить основные виды угроз информационным ресурсам.

8. Охарактеризовать особенности угроз конфиденциальной информации.

9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.

10. Описать причины возникновения каналов несанкционированного доступа к информации.

11. Классифицировать виды каналов несанкционированного доступа к информации.

12. Описать характер действия организационных каналов несанкционированного доступа к информации.

13. Охарактеризовать технические каналы несанкционированного доступа к информации.

14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.

15. Проанализировать особенности угроз автоматизированным информационным системам.

16. Дать классификацию удаленных атак.

17. Проанализировать основные направления правовой защиты информации.

18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.

19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.

20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.

21. Определить объекты защиты авторских прав.

22. Назвать основные права автора в отношении его произведения.

23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).

25. Дать определение государственной тайны и назвать грифы секретности.

26. Перечислить сведения, составляющие государственную тайну и

сведения, которые не могут относиться к государственной тайне.

27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.

28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.

32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

33. Назвать основные положения концепции информационной безопасности предприятия.

34. Изложить содержание регламента обеспечения информационной безопасности предприятия.

35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

42. Проанализировать особенности текста конфиденциального документа.

43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.

44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

45. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.

46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.

47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.

48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.

49. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.

51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. .

52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.

53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

54. Назвать основные элементы физической защиты территории и помещений предприятия.

55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.

56. Дать классификацию компьютерных вирусов.

57. Описать основные антивирусные программы.

58. Охарактеризовать основные способы криптографического преобразования данных.

V. Примерная тематика рефератов:

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность **(**по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений,

относящихся к предпринимательской тайне.

12. Составление инструкции по обработке и хранению конфиденциальных документов.

13. Направления и методы защиты документов на бумажных носителях.

14. Направления и методы защиты машиночитаемых документов.

15. Архивное хранение конфиденциальных документов.

16. Направления и методы защиты аудио- и визуальных документов.

17. Порядок подбора персонала для работы с конфиденциальной информацией.

18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

23. Порядок защиты информации в рекламной и выставочной деятельности.

24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.

31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32. Направления и методы защиты профессиональной тайны.

33. Направления и методы защиты служебной тайны.

34. Направления и методы защиты персональных данных о гражданах.

35. Методы защиты личной и семейной тайны.

7.3.5. Примерный перечень вопросов к зачетам и экзаменам

3-й семестр (зачет)

1. Каким образом десять неформальных свойств модели СВС реализуются в ее формальном описании?
2. В каком случае система (T, s_0) безопасна?
3. Где в определениях безопасности модели СВС реализовано *ss*-свойство безопасности классической модели Белла-ЛаПадулы?
4. Где в определениях безопасности модели СВС реализовано *-свойство безопасности классической модели Белла-ЛаПадулы?
5. Где в определениях безопасности модели СВС реализовано *ds*-свойство безопасности классической модели Белла-ЛаПадулы?
6. Каким стандартам необходимо следовать при построении СУИБ?
7. Что регламентируется в стандарте ISO 27002?
8. Что регламентируется в стандарте ISO 18044?
9. Что должна обеспечивать СУИБ?
10. Какова главная задача СУИБ?
11. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?
12. В каких случаях в КС с мандатным управлением доступом нецелесообразно предотвращение возможности реализации всех информационных потоков от устройств ввода пользователей с высоким уровнем доступа к устройствам вывода пользователей с низким уровнем доступа?
13. В чем отличие информационной невыводимости от информационного невлияния?
14. Почему использование определения требований информационного невлияния (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок?
15. В каких случаях может являться эффективным моделирование безопасности информационных потов с использованием вероятностных подходов?
16. Что понимается под термином информационная безопасность?
17. Что понимается под термином доступность информации?
18. Что понимается под термином целостность информации?
19. Что понимается под термином конфиденциальность информации?
20. Что понимается под термином комплекс средств автоматизации обработки информации?
21. Что понимается под термином информационная безопасность ИС?
22. Что понимается под термином уничтожение информации?
23. Какие способы защиты от вирусов Вы знаете?
24. Какие способы защиты от несанкционированного доступа Вы можете привести?

Какова роль государства в обеспечении компьютерной безопасности?

7.3.6. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Информационная безопасность в системе национальной безопасности Российской Федерации	ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18	Тестирование (Т) Курсовой проект (КП) Зачет
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18	Тестирование (Т) Курсовой проект (КП) Зачет
3	Абстрактные модели обеспечения информационной безопасности	ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18	Тестирование (Т) Курсовой проект (КП) Зачет
4	Основные угрозы информационной безопасности автоматизированных систем	ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18	Тестирование (Т) Курсовой проект (КП) Зачет
5	Основы построения систем защиты информации	ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18	Тестирование (Т) Курсовой проект (КП) Зачет
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	ОК-3, ОПК-4, ОПК-10, ПК-13, ПК-18	Тестирование (Т) Курсовой проект (КП) Зачет

7.4. Порядок процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на этапе промежуточного контроля знаний

Зачет может проводиться по итогам текущей успеваемости и сдачи КР, РГР, КЛ и (или) путем организации специального опроса, проводимого в устной и (или) письменной форме.

Во время проведения экзамена (зачета) обучающиеся могут пользоваться программой дисциплины, а также вычислительной техникой.

8. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), РАЗРАБОТАННОГО НА КАФЕДРЕ

8. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), РАЗРАБОТАННОГО НА КАФЕДРЕ

№ п/п	Наименование издания	Вид издания (учебник, учебное пособие, методические указания, компьютерная программа)	Автор (авторы)	Год издания	Место хранения и количество
1	Информационная безопасность при управлении техническими системами	Учебное пособие	С.А. Баркалов, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов	2015	Библиотека – электр.
2	Средства защиты информации в интегрированных технических системах управления. Методические указания по курсовому проекту	Методические указания	В.Е. Белоусов	2014	Библиотека – электр.
3	Средства защиты информации в интегрированных технических системах управления. Методические указания по самостоятельной работе	Методические указания	В.Е. Белоусов	2014	Библиотека – электр.

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Контрольная работа	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам.
Коллоквиум	Работа с конспектом лекций, подготовка ответов к контрольным вопросам.
Подготовка к зачету	При подготовке к экзамену (зачету) необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и решение задач на практических занятиях.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

10.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля):

10.1.1 Основная литература:

1. Титов А.А. Технические средства защиты информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон.текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 194 с.— Режим доступа: http://www.iprbookshop.ru/13989.

2. *Белоусов В.Е.* Информационная безопасность при управлении техническими системами [Электр]/С.А. Баркалов, В.Е.Белоусов, О.М. Барсуков, К.В. Славнов//Учебное пособие. Воронеж. гос. арх.-строит. ун-т.-Воронеж,.- 365 с.

2. *Белоусов В.Е.* Средства защиты информации в интегрированных технических системах управления. Методические указания для выполнения

курсового проекта [Электронный]// В.Е.Белоусов. Воронеж. гос. арх.–строит. ун–т. -Воронеж, 2014.- 42 с.

3. *Белоусов В.Е.* Средства защиты информации в интегрированных технических системах управления. Методические указания по самостоятельной работе [Электронный]// Е.Белоусов. Воронеж. гос. арх.–строит. ун–т. -Воронеж, 2014.- 33 с.

10.1.2. Дополнительная литература:

4. Алябьева, О. Организация процесса адаптации // Кадровые решения. – 2007. - №6. - С. 81-86.

5. Аминов, В.Л. Кадровая безопасность предприятия // Кадровые решения. – 2009. – № 10. – С.91-99.

6. Бахарева, Е.В. Коммерческая тайна // Секретарь-референт. – 2006. – № 11. – С. 43-50.

7. Громыко, И.А. Общая парадигма защиты информации. Определение терминов: от носителей к каналам утечки информации // Защита информации. Инсайд. – 2008. - № 1. – С.12-15.

8. Доля, А.А. Внутренние ИТ-угрозы в России – 2006 // Защита информации. Инсайд. – 2007. - № 2. – С.60-69.

9. Зенин, Н. Обеспечение конфиденциальности информации – это всегда комплексный подход // Трудовое право. – 2010. – № 1. – С. 41-42.

10. Камаев, В.А., Натров, В.В. Моделирование и анализ состояния информационной безопасности организации // Защита информации. Инсайд. – 2009. - № 4. – С.16-20.

11. Суханова, И.М. Аттестация и комплексная оценка персонала // Кадровые решения. – 2007. - № 4. – С.76-84.

12. Чуковенков, А.Ю. Документы по аттестации служащих // Секретарь-референт. – 2006. - № 11. – С. 17-23.

13. Шубин, А.С. Наша Тайна громко плачет… // Защита информации. Инсайд. – 2008. - № 1. С. 19-27.

14. Янковая, В.Ф. Гриф ограничения доступа к документу // Секретарь-референт. – 2008. - № 1. – С. 17-19.

15. Янковая, В.Ф. Организация конфиденциального делопроизводства // Секретарь-референт. – 2009. - № 12. – С.17 – 20.

Нормативно-правовые источники:

Конституция Российской Федерации // Российская газета. 1993. 25 дек.

О средствах массовой информации. Закон Российской Федерации от 27.12. 1991 № 2124-1// Ведомости съезда народных депутатов РФ и Верховного Совета РФ. - 1992 . - №7. - С. 378 - 399.

Закон Российской Федерации «О безопасности» от 05.03.92 г. // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 15. Ст. 769.

Закон Российской Федерации «О федеральных органах правительственной связи и информации» от 19.02.93 г. №4524-1// Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.1993. №12. Ст.423.

Федеральный закон «О библиотечном деле» от 29.12.94 г. № 78-ФЗ // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 2.

Федеральный закон «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания» от 14.06.94 г. № 5-ФЗ // Собрание законодательства Российской Федерации. 1994. № 8. Ст. 801.

Федеральный закон «О федеральной фельдъегерской связи» от 17.12.94 г. № 67-ФЗ // Собрание законодательства Российской Федерации. № 34. Ст. 3547.

Федеральный закон «Об обязательном экземпляре документов» от 29.12.94 г. № 77-ФЗ // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 1.

Федеральный закон «О рекламе» от 18.07.95 г. № 108-ФЗ // Собрание законодательства Российской Федерации. №30. Ст. 2864.

Федеральный закон «О порядке освещения деятельности органов государственной власти в государственных органах массовой информации» от 13.01.95 г. № 7-ФЗ // Собрание законодательства Российской Федерации. № 3. Ст. 170.

Федеральный закон «О почтовой связи» от 09.08.95 г. № 129-ФЗ // Собрание законодательства Российской Федерации. № 33. Ст. 3334.

Закон Российской Федерации «О государственной тайне» от 21.07.93 г. с изменениями и дополнениями от 06.10.97 г. // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 4673.

Федеральный закон «О связи» от 16.02.95 г. № 15-ФЗ // Собрание законодательства Российской Федерации.1995. №8. № Ст. 600.

Федеральный закон «Об основах государственной службы Российской Федерации» от 31.07.95 г. № 119-ФЗ // Собрание законодательства Российской Федерации. № 31. Ст. 2990.

Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.95 г. № 144-ФЗ// Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

Федеральный закон «Об электронной цифровой подписи» от 10.01.02 г. №1-ФЗ // Собрание законодательства Российской Федерации. 2002. № 2. Ст. 127.

Федеральный закон «О коммерческой тайне» от 09.07.04 г. №98-ФЗ // Собрание законодательства Российской Федерации. 2004. № 32. Ст.3283.

Федеральный закон РФ «Об архивном деле в Российской Федерации» от 22 .10. 2004 . // Собрание Законодательства Российской Федерации. 2004. № 43. Ст. 4169.

Федеральный Закон от 13.03. 2006 . № 38–ФЗ «О рекламе» // Собрание Законодательства Российской Федерации. 2006. № 12. Ст. 1232.

Федеральный Закон от 27.07. 2006 . № 149–ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3448.

Федеральный Закон от 27.07. 2006 . № 152–ФЗ «О персональных данных» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3451.

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред.13.05.2008) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001. № 195-ФЗ (ред.16.05.2008) // Собрание законодательства Российской Федерации. 2002. № 1. (Ч.1). Ст. 1.

Трудовой Кодекс Российской Федерации об от 30.12.2001. № 197-ФЗ (ред.28.02.2008) // Собрание законодательства Российской Федерации. 2002. № 1. (Ч.1). Ст. 3.

Гражданский кодекс Российской Федерации. Часть четвертая от18.12.2006 № 230-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52. Ст. 1232.

Указ Президента Российской Федерации «Об основах государственной политики в сфере информатизации» от 20.01.94 г. № 170 // Собрание актов Президента и Правительства Российской Федерации. 1994. № 4. Ст. 305.

Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» от 30.11.95 г. №1203; в редакции Указа Президента РФ от 24.01.98№ 61 от 06.06.01 г. №659 // Собрание законодательства Российской Федерации. 1998. №5. Ст.561; 2001. №24. Ст.2418.

«Положение о Межведомственной комиссии по защите государственной тайны» утверждено Указом Президента Российской Федерации от 20.01.96 г. №71 // Собрание законодательства Российской Федерации. 1996. № 4. Ст. 268.

Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 // Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.

«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерации 09.09.00 г. №ПР-1895 // Российская газета №187 от 28.09.00 г.

Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 // Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.

Постановление Правительства Российской Федерации «Правила отнесения сведений составляющих государственную тайну, к различным степеням секретности» от 04.09.95 г. № 870 // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

Постановление Правительства Российской Федерации «О государственном учете и регистрации баз и банков данных» от 28.02.99 г. № 226 // Собрание законодательства Российской Федерации. 1999 №12. Ст.1114.

ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, созданным средствами вычислительной техники. М.: Изд-во Стандартов, 1985.

ГОСТ 6.10.1-88. Унифицированные системы документации. Основные положения. М.: Изд-во Стандартов, 1988.

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. М., 1990.

ГОСТ Р-22.0.04-95. Безопасность в чрезвычайных ситуациях. Биолого-социальные чрезвычайные ситуации. Термины и определения. М., 1995.

ГОСТ Р-22.3.05-96. Безопасность в чрезвычайных ситуациях. Жизнеобеспечение населения в чрезвычайных ситуациях. Термины и определения. М.: Изд-во Стандартов, 1996.

ГОСТ Р 50922-96. Защита информации: Основные термины и определения. М., 1996.

ГОСТ Р 6.30-97. Унифицированные системы документации: Система организации норм распорядительной документации: Требования к оформлению документов. М.: Госстандарт. 1998.

ГОСТ 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытания. М.: Изд-во Стандартов, 1999.

ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2000.

ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов. М.: Госстандарт, 2003.

Основные правила работы ведомственных архивов. М., 1988.

10.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем: _

1. Консультирование посредством электронный почты.
2. Использование презентаций при проведении лекционных занятий.

10.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля):

Для работы в сети рекомендуется использовать сайты:

1. научная Электронная Библиотека http://www.e-library.ru;.
2. информационная система «Единое окно доступа к образовательным ресурсам» (http://window.edu.ru/);
3. рекомендуемые поисковые системы http://www.yandex.ru/, http://www.google.ru/, http://www.google.com/ и др.
4. Интернет-библиотека: http://www.twirpx.com
6. Интернет-библиотека: http://www.sciteclibrary.ru

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА:

Компьютерный класс 1305 в составе:

- Рабочие станции – Пентиум -4,8 Ггц – 10 комплектов;
- Принтер лазерный -1 комплект;
- Комплект сетевого оборудования для организации ЛВС и доступа к ресурсам сети ВГАСУ;
- Мультимедиапроектор и экран;
- Программы: Kerio, Антивирус Касперского – 6.0.

Автоматизированные обучающие системы для изучения прикладных программных продуктов, тестирующий комплекс контроля качества обучения, интегрированная система мониторинга хода учебного процесса кафедры.

12. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (образовательные технологии)

Выдача задания на самостоятельную работу осуществляется после проведения «входного» контроля магистрантов приступающих к изучению данной дисциплины на третьей неделе обучения.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к магистрантам. Перед выполнением самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Важным условием успешного освоения дисциплины «Средства защиты информации в интегрированных технических системах управления» является самостоятельная работа студентов. Текущая и опережающая СРС, направленная на углубление и закрепление знаний, а также развитие практических умений заключается в: работе магистрантов с лекционным материалом, поиск и анализ литературы и электронных источников информации по заданной проблеме и выбранной теме магистерской диссертации, выполнении домашних заданий, использовании материалов из тематических информационных ресурсов на иностранных языках, изучении тем, вынесенных на самостоятельную проработку, изучении теоретического материала к индивидуальным заданиям, подготовке к экзамену.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 27.04.04 Управление в технических системах, программа «Системы и средства автоматизации технологических процессов в строительстве».

Руководитель основной
образовательной программы
д.э.н., проф. кафедры
автоматизации технологических
процессов и производств _____/ Е.Н. Десятирикова /

Рабочая программа одобрена учебно-методической комиссией факультета экономики менеджмента и информационных технологий

«3» 09 2018 г., протокол № 1.

Председатель
д. т. н., профессор _____/ П.Н. Курочка /

Эксперт
д.т.н., проф. каф.
информатики и графики ВГТУ _____/А.А. Кононов/