МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» ____02____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы управления информационной безопасностью»

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль
«Кибербезопасность автоматизированных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

степень, звание, должность / И.О. Фамилия /

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»  /А.Ю. Гневшев/

Руководитель образовательной программы,  /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Основы управления информационной безопасностью» следует отнести:

- изучение основных понятий, методологии и практических приемов управления организационной инфраструктурой обеспечения информационной безопасности на предприятии

- подготовка студентов к деятельности в соответствии с квалификационной характеристикой бакалавриата по направлению, формирование у них умений по выбору и построению оптимальной системы защиты информации, внедрению и использованию прогрессивных технологий и средств информационной безопасности, организации их эффективного использования.

К **основным задачам** освоения дисциплины «Основы управления информационной безопасностью» следует отнести:

– приобретение теоретических знания и практических навыков в методике построения и оценки уровня системы защиты информации;

- разработке стратегии обеспечения информационной безопасности и политики ее реализации, разграничении ответственности между подразделениями,

- получение практических навыков управления информационной безопасностью в процессе мониторинга, реагирования на инциденты, аудите системы информационной безопасности на предприятии

Обучение по дисциплине «Основы управления информационной безопасностью» направлено на формирование у обучающихся следующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-2.	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД; ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа Настраивать параметры и сегментировать элементы администрируемой сети ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного

2 Место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к числу учебных обязательных дисциплин основной профессиональной образовательной программы.

«Основы управления информационной безопасностью» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

В базовой и вариативной части цикла:

- организационное и правовое обеспечение информационной безопасности;
- основы информационной безопасности;
- безопасность операционных систем Windows;
- безопасность операционных систем Linox;
- программно-аппаратные средства защиты информации;
- аналитика информационной безопасности.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетных единицы, т.е. **144** академических часа (лабораторные занятия - 72 часа, самостоятельная работа – 72 часа), форма контроля – дифференцированный зачет в 7 семестре.

3.1 Виды учебной работы и трудоемкость (по очной форме обучения)

№ п/п	Вид учебной работы	Количество часов	Семестры	
			7	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**			
	В том числе:			
2.1	Домашние контрольные работы (ДКР)			
3	**Промежуточная аттестация**	**72**	72	
	Экзамен			
	Итого:	**144**	144	

3.2 Тематический план изучения дисциплины (по формам обучения)\

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час		
		Всего	Аудиторная работа	

			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	**Самостоятельная работа**
1	Тема 1. Основные задачи менеджмента в сфере информационной безопасности	22			12		10
2	Тема 2. Роль международных организаций в сфере информационной безопасности	20			10		10
3	Тема 3. Структура государственной системы защиты информации в РФ	22			10		12
4	Тема 4 Управление рисками информационной безопасности	20			10		10
5	Тема 5. Менеджмента в сфере информационной безопасности на уровне предприятий	20			10		10
6	Тема 6. Организация реагирования на чрезвычайные ситуации (инциденты)	20			10		10
7	Тема 7. Аудит состояния информационной безопасности предприятия.	20			10		10
Итого		**144**			**72**		**72**

3.3 Содержание дисциплины

Тема 1. Основные задачи менеджмента в сфере информационной безопасности

Классификация и перечень факторов, воздействующих на безопасность защищаемой информации (Гост PS 1275). Задачи управления информационной безопасностью. Понятие безопасной информационной инфраструктуры и ее составляющие. Уровни организационной работы в сфере информационной безопасности

Тема 2. Роль международных организаций в сфере информационной безопасности

Основные организационные принципы, направления деятельности международных профессиональных объединений в сфере информационной безопасности. Направления организационной работы специализированных международных организаций и объединений. Организационная деятельность в сфере ИБ альянсов крупных технологических компаний. Внешняя и внутренняя организационная работы корпорации Microsoft в сфере информационной безопасности

Тема 3. Структура государственной системы защиты информации в РФ

Основополагающие документы, определяющие политику РФ в сфере информатизации и обеспечения защиты информации. Функции, выполняемые организациями, входящими в государственную систему защиты информации.

Тема 4. Управление рисками информационной безопасности

Основные понятия и определения управления информационными рисками. Процесс управления рисками информационной безопасности. Описание внешних и внутренних условий, в которых функционирует организация, определение целей управления рисками, определение критерия оценки и приемлемости риска Шкала ценности активов. Количественные, качественные и смешанные методы оценки рисков. Шкалы вероятности угроз и уязвимостей, Оценка уровня риска выявление существующих контролей (контрмер). Этапы обработки риска. Управление информационными рисками, стандарты, нормативные документы, рекомендации. Программные средства, используемые для анализа и управления рисками.

Тема 5. Менеджмента в сфере информационной безопасности на уровне предприятий

Структура организационной деятельности по обеспечению информационной безопасности на уровне предприятия. Структура политики информационной безопасности и процесс ее разработки. Содержание политики информационной безопасности предприятия верхнего и среднего уровня. Детализированные политики безопасности. Задачи департамента информационной безопасности. Организационная работа с персоналом

Тема 6. Организация реагирования на чрезвычайные ситуации (инциденты)

Нормативные документы, регламентирующих аспекты управления инцидентами информационной безопасности. Процедуры и этапы реагирования на инциденты. Локализация и устранение последствий инцидента. Анализ процесса нападения и его обстоятельств

Тема 7. Аудит состояния информационной безопасности предприятия.

Цель аудита. Этапы аудита информационной безопасности. Методики оценки рисков информационной безопасности. Содержание аудиторской проверки. Понятие инструментального контроля. Содержание отчета о результатах аудита состояния ИБ предприятия

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

2. Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденный Приказом Министерства образования и науки РФ от 19 сентября 2017 г. N 929 "Об утверждении федерального… Редакция с изменениями N 1456 от 26.11.2020

3. Приказ Министерства образования и науки РФ от 05 апреля 2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры;

4. Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Минобрнауки России от 29 июня 2015 г. № 636;

5. Положение о практической подготовке обучающихся, утвержденное приказом Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 5 августа 2020 г. № 885/390;

6. Устав и локальные нормативные акты Московского политехнического университета.

Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата (далее - выпускники), могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сфере проектирования, разработки, внедрения и эксплуатации средств вычислительной техники и информационных систем, управления их жизненным циклом).

Выпускники могут осуществлять профессиональную деятельность в других областях и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника, предъявляемым соответствующими профессиональными стандартами.

4.2 Основная литература

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3448 — Режим доступа: http://www.szrf.ru/doc.phtml?nb=edition00&issid=2006031000&docid=104
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005.
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006.
4. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 .

4.2 **Дополнительная литература**

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с. - ISBN 5-93517-292-5 : 204-33. Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 5-93517-292-5. (25 экз.)
2. Курс экономической теории. Учебник/Под ред. М.Н. Чепурина, Е.А. Киселевой. Киров, 2012. -752 с.
3. Мельников В.В. Государственное регулирование национальной экономики. Учебное пособие. М.: Омега-Л, 2012. -120 с.
4. Астахов А.М. Искусство управления информационными рисками –М.: ДМК Пресс, 2010. **(10 экз.)**
5. Конев А.А., Давыдова Е.М., Шелупанов А.А. Управление информационной безопасностью: лабораторный практикум. – Томск: В-Спектр, 2017.

6. Ларина И.Е. Экономика защиты информации. Учебное пособие.; МГИУ, 2007 г – 96 с
7. Нестеров С.А. Основы информационной безопасности: Учебное пособие:- СПб.: Издательство Политехнического университета, 2014г. Режим доступа: http://biblioclub.ru

4.4 Электронные образовательные ресурсы

1. 1. STAFFCopp DLP-система (Пилотный проект)
2. Журнал «информационная безопасность» Режим доступа :http://itsec.ru/imag/

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. OS Linux mint.
2. Apache OpenOffice.
3. Веб-браузеры, Chrome, Firefox.
4. Gimp.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Федеральная государственная информационная система - Национальная электронная библиотека (НЭБ) https://нэб.рф

8. Материально-техническое обеспечение

Проведение лекционных и практических осуществляется в мультимедийной аудитории.

9. Методические рекомендации

a. Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

b. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *аудиторные занятия, лабораторные работы.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты и записи, готовятся к

промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях, промежуточный контроль осуществляется на дифференцированном зачете в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Фонд оценочных средств

a. Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- подготовка и выступление на семинарском занятии с презентацией и обсуждением по темам рефератов и творческих заданий;

-контрольные вопросы и задания в форме бланкового и (или) компьютерного тестирования,

-контрольные работы для контроля освоения обучающимися разделов дисциплины,

- подготовка к выполнению лабораторных работ и их защита,

- дифференцированный зачет.

Лабораторные работы представляют собой работы, предусматривающие реализацию приобретенных теоретических и практических навыков, обучающихся по направлению в вопросах метрологии построения, организации функционирования и управления системой информационной безопасности информационной системы предприятия.

Образцы тестовых заданий, контрольных работ для проведения текущего контроля, тем рефератов, вопросов к дифференцированному зачету, приведены в приложении.

b. Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	Критерии оценивания			
	2	3	4	5
ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения				
ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД; ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа Настраивать параметры и сегментировать элементы администрируемой сети ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного				

Шкала оценивания результатов промежуточной аттестации и её описание:

Форма промежуточной аттестации: дифференцированный зачет.

Промежуточная аттестация обучающихся в форме дифференцированного зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине – выполнение и защита контрольных работ согласно полученному заданию с достижением порогового значения оценки.

Шкала оценивания	Описание
Отлично	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 5. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 4. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент

	демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 3. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не достигнуто пороговое значение хотя бы для одного уровня формируемых на момент проведения аттестации компетенций. Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

с. Оценочные средства

1. Примерные темы рефератов, но курсу **««Основы управления иформационной безопасностью»**

1.Безопасность и правовое регулирование электронной коммерции
2. Обзор деятельности центров реагирования на инциденты в РФ
3. Обзор деятельности МСЭТ по управлению информационной безопасности
4.Обзор материалов Гост Р ИСО/МЭК 18044 -2007 Менеджмент инцидентов информационной безопасности
5. Обзор материалов Гост ISO/IEC 27005-2012 Методы обеспечение безопасности. Менеджмент рисков безопасности
6. Менеджмент непрерывности бизнеса
7. Менеджмент оказание услуг третьим лицам и клиентам
8. Направления организационной работы в области безопасности, связанной с персоналом.
9. Оценка эффективности передачи риска информационной безопасности третьим лицам
10 Мониторинг безопасности
11 Задачи департамента информационной безопасности
12 Аудит безопасности информационных технологий

2. Тестовые вопросы по курсу **«Основы управления информационной безопасностью»**

Тест 1.

1. Меры защиты информационной безопасности направлены на защиту от:
1 нанесения неприемлемого ущерба;
2. нанесения любого ущерба;
3. вандализма.

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

1. доступность;
2. целостность;
3. конфиденциальность;
4. правдивое отражение действительности.

3. Что такое защита информации?

1. защита от несанкционированного доступа к информации;
2. выпуск бронированных упаковок для дисков;
3.комплекс мероприятий, направленных на обеспечение информационной безопасности.

4 Что понимается под информационной безопасностью?

1.защита здоровья персонала;
2.защита от нанесения неприемлемого ущерба субъектам информационных отношений;
3.обеспечение информационной независимости России.

5. Самыми опасными угрозами являются:

1. непреднамеренные ошибки штатных сотрудников;
2. вирусные инфекции;
3. атаки хакеров.

6. Дублирование сообщений является угрозой:

1. доступности;
2.конфиденциальности;
3. целостности.

7. Агрессивное потребление ресурсов является угрозой:

1.доступности;
2.конфиденциальности;
3.целостности.

8. Согласно Закону «Об информации, информатизации и защите Информации» персональные данные – это:

1.сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
2. данные, хранящиеся в персональном компьютере;
3. данные, находящиеся в чьей-либо персональной собственности.

9. Что нельзя отнести к функциям, выполняемым службой защиты информации:

1. финансовое обеспечение деятельности организации;
2. организация обучения персонала правилам соблюдения и поддержания
3.информационной безопасной деятельности предприятия;
4. материально-техническое и технологическое обеспечение информационной безопасности на предприятии.

10. Главная цель мер по защите информации, предпринимаемых на административном уровне:

1. сформировать программу безопасности и обеспечить еѐ выполнение;
2. выполнить положения действующего законодательства;
3 отчитаться перед вышестоящими инстанциями.

11. В число целей политики безопасности верхнего уровня входит:
1. решение сформировать или пересмотреть комплексную программу безопасности;
2.обеспечение базы для соблюдения законов и правил;
3. обеспечение конфиденциальности почтовых сообщений.

12. Какие виды страхования в рамках системы защиты информации возможны
1. страхование имущества и личное страхование;
2. страхование имущества, ответственности и личное страхование;
3. страхование имущества и ответственности.

13. В число этапов жизненного цикла информационного сервиса входят:
1.закупка;
2.продажа;
3.выведение из эксплуатации.

14.Ущерб от различных рисков потери информации включает
1. прямые и косвенные убытки;
2. упущенную выгоду предприятия от простоя атакованного узла;
3. прямые убытки от понесенного ущерба.

Тест 2

1. Политика безопасности:
1.фиксирует правила разграничения доступа;
2.отражает подход организации к защите своих информационных активов;
3. описывает способы защиты руководства организации.

2.В число этапов процесса планирования восстановительных работ после реализации угроз входят:
1.выявление критически важных функций организации;
2.определения перечня возможных аварий;
3. проведение тестовых аварий.

3.В число принципов физической защиты входят:
1.беспощадный отпор;
2.непрерывность защиты в пространстве и времени;
3.минимизация защитных средств.

4. При оценке рисков информационной безопасности не по двум, а по трем факторам какой дополнительный фактор учитывается
1. цена потери;
2. вероятность происшествия;
3. вероятность угрозы.

5. К какому способу воздействия на риск относится способ страхование рисков
1. исключение риска
2. снижения вероятности возникновения риска
3. сохранение существующего уровня риска

6. Мониторинг, протоколирование и аудит могут использоваться для:
1. предупреждения нарушений ИБ;
2. обнаружение нарушений;
3. восстановление режима ИБ.

7. В число основных принципов архитектурной безопасности входят:
1.применение наиболее передовых технических решений;
2. применение простых апробированных решений;
3.сочетание простых и сложных защитных средств.

8. Контроль целостности может использоваться для:
1. предупреждения нарушений информационной безопасности;
2.обнаружения нарушений;
3.локализации последствий нарушений.

9.Обеспечение высокой доступности можно ограничить:
1.критически важными серверами;
2.сетевым оборудованием;
3. всей цепочкой от пользователей до серверов.

10 Предметная область «Защита информации» согласно ГОСТ Р 50922-96 – это:
1. деятельность (процесс), направленная на предотвращение утечки защищаемой информации;
2.специализаированная организация;
3.это самостоятельное структурное подразделение в рамках деятельности организации, тесно связана со службами охраны и объектового режима, составляет основу всей системы обеспечения информационной безопасности.

11. К организационным задачам и функциям службы защиты информации не относится:
1. разработка проектов защиты для каждого вида безопасности их реализация приемка и контроль их постоянной работоспособности;
2. организация проведения совместно с другими подразделениями мероприятий в отношении конкурентов,
3. взаимодействия с правоохранительными органами;
4. оказание управленческих воздействий на создание/поддержку своевременной реорганизации структуры управления безопасности предприятия.

12. Каковы требования к технологии управления безопасностью?
1.соответствие современному уровню развития информационных технологий;
2. выделение максимально возможных средств на защиту информации;
3. наличие обособленных субъектов в информационной системе.

13. На чем должно базироваться правовое обеспечение информационной безопасности:
1. соблюдение принципов законности;
2. комплексности и индивидуальности;
3. системности подходов;
4. балансе интересов в информационной сфере.

14. Действия Закона -О лицензировании отдельных видов деятельности‖ не распространяется на:
1.деятельность по технической защите конфиденциальной информации;
2.образовательную деятельность в области защиты информации;
3.предоставление услуг в области шифрования информации.

3. Варианты контрольных работ

1. Контрольная работа 1. «Правовые основы построения системы защиты информации и оценка рисков».

Вариант 1.

Задание 1. Структура государственной системы защиты информации.

Задание 2. Идентификация рисков работы со сторонними организациями.

Вариант 2.

Задание 1. Основные документы, определяющие политику РФ в сфере информационной безопасности.

Задание 2. Методика оценки рисков информационной безопасности по двум и трем факторами.

2. **Контрольная работа 2.** «Мониторинг безопасности и реагирование на инциденты»

Вариант 1.

Задание 1. Цели аудита состояния информационной безопасности

Задание 2. Этапы процесса реагирования на инциденты

Вариант 2.

Задание. 1 Этапы проведения аудита информационной безопасности

Задание 2. Процедуры идентификация нападающего в процессе реагирования на инцидент

4. Творческое задание

Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания в области управления информационной безопасностью информации и аргументировать собственную точку зрения. Выполняется группой обучающихся из 3-4 человек. Тема творческого задания: «Разработка политики безопасности локального и нижнего уровней на экономическом объекте». В качестве объекта исследования группа выбирает и описывает виртуальное предприятие, работающего в различных областях и занимающегося различными сферами деятельности (государственное образовательное учреждение, адвокатская контора, предприятие, занимающееся электронной коммерцией, предприятие связи, поликлиника, аутсорсинговая компания, страховая компания, банк).

Содержание творческого задания

1. Описание хозяйственной деятельности выбранного объекта защиты, положения на рынке, конкуренты, контрагенты, клиенты, перечень предоставляемых услуг.
2. Построение модели угроз и нарушителя информационной безопасности
3. Оценка уровня защищенности выбранного предприятия
4. Разработка политики безопасности верхнего уровня
5. Разработка политики безопасности среднего уровня по направлениям (менеджмент активов, физическая безопасность, безопасность финансовой деятельности, управление доступом, менеджмент непрерывности бизнеса, менеджмент инцидентов)

6. Разработка должностной инструкции специалиста- пользователя информационными ресурсами предприятия

5 Контрольные вопросы к экзамену по дисциплине «Основы управления информационной безопасностью»

1. Классификация и перечень факторов, воздействующих на безопасность защищаемой информации (ГОСТ Р51275)
2. Основные задачи менеджмента в сфере информационной безопасности
3. Понятие безопасной информационной инфраструктуры и ее составляющие
4. Уровни организационной работы в сфере информационной безопасности
5. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности
6. Роль международных организаций и объединений в сфере информационной безопасности
7. Обзор деятельности международных профессиональных объединений и направлений их деятельности в сфере информационной безопасности
8. Направления организационной работы в сфере информационной безопасности специализированных международных организаций и объединений
9. Роль и направления деятельности альянсов крупных технологических компаний в сфере информационной безопасности
10. Направление внутренней организационной работы в сфере информационной безопасности корпорации Microsoft
11. Направления внешней организационной работы корпорации Microsoft в сфере информационной безопасности
12. Особенности организационной деятельности государства в сфере информационной безопасности
13. Основополагающие документы, определяющие политику РФ в сфере информатизации и обеспечения защиты информации
14. Структура государственной системы защиты информации в РФ
15. Функции, выполняемые организациями, входящими в государственную систему защиты информации
16. Предпосылки развития менеджмента в сфере информационной безопасности на уровне предприятий
17. Структура организационной деятельности по обеспечению информационной безопасности на уровне предприятия
18. Структура политики информационной безопасности и процесс ее разработки
19. Содержание политики информационной безопасности предприятия верхнего и среднего уровня
20. Задачи департамента информационной безопасности предприятия
21. Организационная структура департамента информационной безопасности и функции, выполняемые его отделами
22. Направления организационной работы в области безопасности, связанной с персоналом
23. Меры по организации физической безопасности и защиты от воздействия окружающей среды
24. Организационные аспекты безопасности взаимодействия со сторонними организациями (клиентами)
25. Менеджмент оказания услуг третьим лицам
26. Мероприятия по обеспечению безопасности использования мобильной вычислительной техники
27. Менеджмент непрерывности бизнеса
28. Мониторинг безопасности
29. Этапы процесса реагирования на инциденты
30. Реагирования на инциденты- этап обнаружение нападения

31. Реагирование на инциденты – локализация и устранение последствий нападения
32. Реагирование на инциденты – этап идентификации нападающего
33. Реагирование на инциденты – этап оценки и анализа процесса нападения и его обстоятельств
34. Организация и цели аудита состояния информационной безопасности предприятия
35. Этапы и стадии аудита информационной безопасности
36. Содержание отчета о результатах аудита состояния информационной безопасности предприятия