Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 07.11.2023 18:10:48
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы управления информационной безопасностью»

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль
«Безопасность компьютерных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2022 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

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 4
2 Место дисциплины в структуре образовательной программы 6
3 Структура и содержание дисциплины 6
3.1 Виды учебной работы и трудоемкость 6
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 7
4 Учебно-методическое и информационное обеспечение 8
4.1 Основная литература 8
4.2 Дополнительная литература 9
4.3 Электронные образовательные ресурсы 9
5 Материально-техническое обеспечение 9
5.1 Требования к оборудованию и помещению для занятий 9
5.2 Требования к программному обеспечению 9
6 Методические рекомендации 9
6.1 Методические рекомендации для преподавателя по организации обучения 9
6.2 Методические указания для обучающихся по освоению дисциплины 9
7 Фонд оценочных средств 11
7.1 Методы контроля и оценивания результатов обучения 11
7.2 Шкала и критерии оценивания результатов обучения 11
7.3 Оценочные средства 17
7.3.1 Примерные темы рефератов. 17
7.3.2 Тестовые вопросы. 18
7.3.3 Варианты контрольных работ. 21
7.3.4 Контрольные вопросы к экзамену по дисциплине. 23

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 «Организация ЭВМ и вычислительных систем» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	**знать:** -основные угрозы безопасности и модели нарушителя информационной безопасности; **владеть:** -навыками анализа информационной инфраструктуры, выявления угроз информационной безопасности объекта информатизации и демонстрировать способность и готовность к выбору комплекса средств и обоснованию критериев эффективности функционирования систем защиты информации на предприятии
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по	**знать:** - принципы формирования общих и детализированных политик информационной безопасности

обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	
ПК-2. Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**владеть:** - методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности
ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**уметь:** -оценивать информационные риски, проводить внутренний аудит состояния, работоспособности и эффективности применяемых средств и методов защиты информации.
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	**уметь:** - составлять аналитические обзоры, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии
ПК-8. Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**знать:** - существующие стандарты и методологии по управлению информационной безопасностью; **уметь:** - анализировать текущее состояние защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности;
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	**уметь:** - контролировать эффективность принятых мер по реализации политик безопасности
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской	**знать:** - нормативные правовые акты и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **уметь:**

Федерации, Федеральной службы по техническому и экспортному контролю	- разрабатывать политики организации безопасного доступа к информации ограниченного пользования

2 Место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к числу профессиональных учебных дисциплин обязательной части (Б1.1) основной образовательной программы бакалавриата (Б1.1.41).

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

В базовой и вариативной части цикла (Б1):

- организация и правовое обеспечение информационной безопасности;
- основы информационной безопасности;
- безопасность операционных систем;
- программно-аппаратные средства защиты информационной безопасности;
-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 – экзамен в 7 семестре.

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	7	1-18
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	7	1-18
2	**Самостоятельная работа**	**36**	7	1-18
3	**Промежуточная аттестация**		7	19
	Экзамен		7	19
	Итого:	**108**		

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				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Основные понятия и анализ угроз информационной безопасности	18			12		6
2	Раздел 2. Проблемы информационной безопасности сетей	12			8		4
3	Раздел 3. Политика безопасности	15			10		5
4	Раздел 4. Криптографическая защита информации	18			12		6
5	Раздел 5. Технологии аутентификации	12			8		4
6	Раздел 6. Технологии межсетевых экранов	9			6		3
7	Раздел 7. Технологии защиты от вирусов	9			6		3
8	Раздел 8. Требования к системам защиты информации	9			6		3
9	Раздел 9. Основы правового обеспечения защиты информации	6			4		2
Итого		**108**			**72**		**36**

3.3 Содержание дисциплины

Раздел 1. Основные понятия и анализ угроз информационной безопасности.

Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности.

Раздел 2. Проблемы информационной безопасности сетей

Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг.

Раздел 3. Политика безопасности

Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности.

Раздел 4. Криптографическая защита информации

Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные криптосистемы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП).

Раздел 5. Технологии аутентификации

Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода.

Раздел 6. Технологии межсетевых экранов

Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий.

Раздел 7. Технологии защиты от вирусов

Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ.

Раздел 8. Требования к системам защиты информации

Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных.

Раздел 9. Основы правового обеспечения защиты информации

Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности.

3.4.1 Лабораторные работы

Раздел 1. Основные понятия и анализ угроз информационной безопасности.

Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.

Раздел 2. Проблемы информационной безопасности сетей

Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.

Раздел 3. Политика безопасности

Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети

Раздел 4. Криптографическая защита информации

Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.

Раздел 5. Технологии аутентификации

Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.

Раздел 6. Технологии межсетевых экранов

Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.

Раздел 7. Технологии защиты от вирусов

Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.

Раздел 8. Требования к системам защиты информации

Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

Раздел 9. Основы правового обеспечения защиты информации

Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

4 Учебно-методическое и информационное обеспечение

4.1 Основная литература

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 22.05.2022). – Режим доступа: по подписке. – Текст: электронный
2. Горбунов, А. В. Проектирование защищённых оптических теле-коммуникационных систем : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 22.05.2022). – Режим доступа: по подписке. – Текст: электронный..

4.2 Дополнительная литература

1. Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. – Воронеж : Во- ронежский государственный университет инженерных технологий, 2012. – 172 с. – URL: https://biblioclub.ru/index.php?page=book&id=141626 (дата обращения: 22.05.2022). – Режим доступа: по подписке. – Текст : электронный
2. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 222 с. – URL: https://biblioclub.ru/index.php?page=book&id=458204 (дата обращения: 22.05.2022). – Режим доступа: по подписке. – Текст : электронныйАстахов А.М. Искусство управления информационными рисками –М.: ДМК Пресс, 2010. **(10 экз.)**

3. Конев А.А., Давыдова Е.М., Шелупанов А.А. Управление информационной безопасностью: лабораторный практикум. – Томск: В-Спектр, 2017.
4. Ларина И.Е. Экономика защиты информации. Учебное пособие.; МГИУ, 2007 г – 96 с
5. Нестеров С.А. Основы информационной безопасности: Учебное пособие:- СПб.: Издательство Политехнического университета, 2014г. Режим доступа: http://biblioclub.ru

4.3 Электронные образовательные ресурсы

1. ЭОР разрабатывается
2. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
3. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
4. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
5. Электронно-библиотечная система IQLib – http://www.iqlib.ru
6. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

5 Материально-техническое обеспечение

5.1 Требования к оборудованию и помещению для занятий

Для проведения лабораторных работ и самостоятельной работы студентов подходят аудитории, оснащенные компьютерами с программным обеспечением в соответствии со списком в пункте 4.5 и подключенные к интернету.

Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

Рабочее место преподавателя должно быть оснащено компьютером с подключенным к нему проектором или иным аналогичным по функциональному назначению оборудованием.

5.2 Требования к программному обеспечению

1. Операционная система Windows 10(или ниже) - MicrosoftOpenLicense
   Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215
2. Офисные приложения, MicrosoftOffice 2013(или ниже) - MicrosoftOpenLicense
   Лицензия № 61984042
3. STAFFCopp DLP-система (Пилотный проект)
4. Журнал «информационная безопасность» Режим доступа :http://itsec.ru/imag/

6 Методические рекомендации

6.1 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.

6.2 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 *лекции.* При рассмотрении учебного материалы рекомендуется делать акцент на структуру и взаимосвязь аспектов безопасности - методологии, информационного обеспечения, нормативно-правовой базы, организации управления, кадрового обеспечения, аудита состояния информационной безопасности экономического объекта. Полезно также сосредоточить внимание студентов на анализе угроз и оценке рисков информационной безопасности, оценке прямого и косвенного ущерба от риска потери информации, определении упущенной выгоды предприятия.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы. Преподаватель направляет самостоятельную работу студентов, отвечает на возникающие вопросы, дает рекомендации по методике изучения тем.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Практические занятия* проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине «Основы управления информационной безопасностью» предполагает: подготовку реферата с презентацией, а также выполнение

студентами самостоятельного, частично регламентированного задания, имеющего нестандартное решение и позволяющее диагностировать умения, интегрировать знания в области управления информационной безопасностью критически важной информации и аргументировать собственную точку зрения. Тема творческого задания: «Разработка политики безопасности локального и нижнего уровней на экономическом объекте». ТЗ являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами 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 студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Творческое задание выполняется индивидуально или в группах из 3-4 человек.

Контроль самостоятельной работы организуется в двух формах:

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

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность умений.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в устной форме.

7 Фонд оценочных средств

7.1 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,

- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине «Основы управления информационной безопасностью»

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: -основные угрозы безопасности и модели нарушителя информационной безопасности	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие знаний в области основных угроз и модели нарушителя информационной безопасности	Обучающийся демонстрирует неполное знание в области основных угроз безопасности и модели нарушителя информационной безопасности,	Обучающийся демонстрирует частичные знания в области основных угроз безопасности и модели нарушителя информационной безопасности, но допускаются незначительные ошибки, неточности, затруднения при аналитических ситуациях.	Обучающийся демонстрирует полные знания в области основных угроз безопасности и модели нарушителя информационной безопасности, и свободно оперирует приобретенными знаниями.
владеть: -навыками анализа информационной инфраструктуры, выявления угроз информационной безопасности объекта информатизации и демонстрировать способность и готовность к выбору комплекса средств и обоснованию критериев эффективности функционирования систем защиты информации на предприятии	Обучающийся не владеет или в недостаточной степени владеет навыками анализа информационной инфраструктуры, выявления угроз и оценки рисков информационной безопасности объекта информатизации и не могут демонстрировать способность и готовность к выбору комплекса средств и обоснованию критериев эффективности функционирования	Обучающийся владеет методиками информационной инфраструктуры, выявления угроз и оценки рисков информационной безопасности объекта информатизации в неполном объеме, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду методик испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет методами анализа информационной инфраструктуры, выявления угроз и оценки рисков информационной безопасности объекта информатизации, но допускаются незначительные ошибки, затруднения при -переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет методами анализа информационной инфраструктуры, выявления угроз и оценки рисков информационной безопасности объекта информатизации, свободно применяет полученные навыки в ситуациях повышенной сложности

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты				
знать: - принципы формирования общих и детализированных политик информационной безопасности	Обучающийся демонстрирует полное отсутствие или недостаточное знание прин-ципов формирования общих и детализированных политик информационной безопасности	Обучающийся демонстрирует неполное соответствие знаний принципов формирования общих и детализированных политик информационной безопасности, испытываются значительные затруднения при применении знаний в новых ситуациях	Обучающийся демонстрирует частичное соответствие знаний принципов формирования общих и детализированных политик информационной безопасности, но допускает незначительные ошибки, неточности, затруднения при аналитических ситуациях	Обучающийся демонстрирует полное соответствие знаний принципов формирования общих и детализированных политик информационной безопасности, и свободно оперирует приобретенными знаниями
ПК-2 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
Владеть: - методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности	Обучающийся не владеет или в недостаточной степени владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности	Обучающийся владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности в неполном объеме, допускаются значительные ошибки, испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности, навыки освоены, но допускаются незначительные ошибки, затруднения при переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности свободно применяет полученные навыки в ситуациях повышенной сложности
ПК-3 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				

уметь: - оценивать информационные риски, проводить внутренний аудит состояния, работоспособности и эффективности применяемых средств и методов защиты информации автоматизированных систем.	Обучающийся не умеет или в недостаточной степени умеет оценивать информационные риски и не может провести внутренний аудит состояния, работоспособности и эффективности применяемых средств и методов защиты информации автоматизированных систем.	Обучающийся демонстрирует неполное соответствие умению оценивать информационные риски и проведению внутреннего аудита состояния, работоспособности и эффективности применяемых средств и методов защиты информации автоматизированных систем. испытываются значительные затруднения при применении навыков в новых ситуациях	Обучающийся демонстрирует частичное умение в оценке рисков и по проведении внутреннего аудита состояния, работоспособности и эффективности применяемых средств и методов защиты информации автоматизированных систем, допускает незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений в оценке рисков и проведении аудита состояния, работоспособности и эффективности применяемых средств и методов защиты информации автоматизированных систем, свободно оперирует приобретенным умениями, применяет их в ситуациях повышенной сложности.
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений				
уметь: - оставлять аналитические обзоры, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии ,	Обучающийся не умеет или в недостаточной степени умеет составлять аналитические обзоры, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии.	Обучающийся демонстрирует неполное соответствие умению составлять аналитические обзоры, систематизировать научно-техническую и нормативную информацию, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии, испытываются значительные затруднения при применении навыков в новых ситуациях	Обучающийся демонстрирует частичное умение по составлению аналитических обзоров, систематизации научно-технической и нормативной информации, разработки предложений по совершенствованию системы управления информационной безопасностью на предприятии, допускает незначительные ошибки, неточности, затруднения при переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умению составлять аналитические обзоры, систематизировать научно-техническую и нормативную информацию, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии, свободно оперирует приобретенным умениями, применяет их в ситуациях повышенной сложности

ПК-8 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
знать: - существующие стандарты и методологии по управлению информационной безопасностью,	Обучающийся демонстрирует полное отсутствие или недостаточное знание существующих стандартов и методологии по управлению информационной безопасностью,	Обучающийся демонстрирует неполное знание существующих стандартов и методологии по управлению информационной безопасностью, испытываются значительные затруднения при применении навыков в новых ситуациях	Обучающийся демонстрирует частичное знание стандартов и методологии по управлению информационной безопасностью, но допускает незначительные ошибки, неточности, затруднения при аналитических ситуациях	Обучающийся демонстрирует полное соответствие знаний стандартов и методологии по управлению информационной безопасностью, и свободно оперирует приобретенными знаниями.
уметь: - анализировать текущее состояние защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности;	Обучающийся не умеет или в недостаточной степени умеет анализировать текущее состояния защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности	Обучающийся демонстрирует неполное соответствие умению проводить анализ текущего состояния защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности	Обучающийся демонстрирует частичное умение по проведению анализа текущего состояния защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности,	Обучающийся демонстрирует полное соответствие умению в проведении анализа текущего состояния защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности
ПК-6 Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
Уметь: - контролировать эффективность принятых мер по реализации политик безопасности	Обучающийся не умеет или в недостаточной степени умеет контролировать эффективность принятых мер по реализации политик безопасности	Обучающийся демонстрирует неполное умение в осуществлении контроля эффективность принятых мер по реализации политик безопасности, допускаются значительные ошибки,	Обучающийся демонстрирует частичное умение в осуществлении контроля эффективности принятых мер по реализации политик безопасности, навыки освоены, но допускаются незначительные	Обучающийся демонстрирует полное умение в осуществлении контроля эффективность принятых мер по реализации политик безопасности, свободно применяет полученные навыки в ситуациях

		испытываются значительные затруднения при применении навыков в новых ситуациях	ошибки, затруднения при переносе умений на новые, нестандартные ситуации.	повышенной сложности
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
знать: - нормативные правовые акты и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Обучающийся демонстрирует полное отсутствие или недостаточное знание существующих нормативных правовых актов и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Обучающийся демонстрирует неполное знание существующих нормативных правовые актов и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Обучающийся демонстрирует частичное знание, нормативных правовые актов и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, но допускает незначительные ошибки, неточности, затруднения при их применении	Обучающийся демонстрирует полное соответствие знаний нормативных правовые актов и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю и свободно оперирует приобретенными знаниями.
уметь: - разрабатывать политики организации безопасности доступа к информации ограниченного пользования	Обучающийся не умеет или в недостаточной степени умеет разрабатывать политики организации безопасности доступа к информации ограниченного пользования и контролировать их применение	Обучающийся демонстрирует в недостаточном объеме умение по разработке политики безопасности доступа к информации ограниченного пользования и контроле их применения, допускаются значительные ошибки, испытываются значительные затруднения при применении навыков в новых ситуациях	Обучающийся демонстрирует частичное умение в разработке политики безопасности доступа к информации ограниченного пользования и контролю их применение, допускает незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное умение в разработке политики безопасности доступа к информации ограниченного пользования и контроля их применение, свободно оперирует приобретенным умениями, применяет их в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине, при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине 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 (выполнили контрольные работы, выступили на семинаре с презентацией, предоставили реферат, защитили лабораторные работы)

Шкала оценивания	***Описание***
Отлично	*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	*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	*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 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.

7.3 Оценочные средства

7.3.1 Примерные темы рефератов.

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

7.3.2 Тестовые вопросы.

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**.**

7.3.3 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

7.3.4 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