

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 30.10.2025 12:49:45
Уникальный программный ключ:
8db180d1a3f02ac9e807113671742935e1864e

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

УТВЕРЖДЕНО

Декан факультета

Информационных технологий



/ А.Ю. Филиппович /

«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы управления информационной безопасностью»

Направление подготовки

10.03.01 «Информационная безопасность»

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная

Год приема 2020

Москва 2020 г.

1. Цели освоения дисциплины.

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

2. Место дисциплины в структуре ООП бакалавриата.

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

«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.Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
-----------------	---	---

ОПК - 7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	<p>знать: -основные угрозы безопасности и модели нарушителя информационной безопасности;</p> <p>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</p>
ПК - 4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	<p>знать: - принципы формирования общих и детализированных политик информационной безопасности</p>
ПК – 5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	<p>владеть: - методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности</p>
ПК – 6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	<p>уметь: -оценивать информационные риски, проводить внутренний аудит состояния, работоспособности и эффективности применяемых средств и методов защиты информации.</p>
ПК – 7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	<p>уметь: - составлять аналитические обзоры, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии</p>
ПК - 10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	<p>знать: - существующие стандарты и методологии по управлению информационной безопасностью;</p> <p>уметь: - анализировать текущее состояние защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности;</p>

ПК - 13	способностью 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
ПК - 15	способностью 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: - нормативные правовые акты и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю уметь: - разрабатывать политики организации безопасного доступа к информации ограниченного пользования

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет **4** зачетных единицы, т.е. **144** академических часа (лекции – 36 часов, практические занятия – 0 часов, лабораторные занятия - 36 час, самостоятельная работа – 72 часа), форма контроля – экзамен в 7 семестре.

Структура и содержание дисциплины «Основы управления информационной безопасностью» по срокам и видам работы отражены в приложении.

Содержание разделов 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, регламентирующие 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

5. Образовательные технологии.

Методика преподавания дисциплины «Основы управления информационной безопасностью» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся:

- подготовка к выполнению лабораторных работ;
- обсуждение и защита рефератов и творческих заданий по дисциплине;
- подготовка, представление и обсуждение презентаций по темам рефератов на семинарских занятиях;
- организация и проведение текущего контроля знаний студентов в форме бланкового тестирования;
- проведение мастер-классов экспертов и специалистов по методам и средствам мониторинга, аудита и оценки затрат на функционирования системы защиты информации

Удельный вес занятий, проводимых в интерактивных формах, определен главной целью образовательной программы, особенностью контингента обучающихся, содержанием дисциплины «Основы управления информационной безопасностью» и в целом по дисциплине составляет 25%

аудиторных занятий. Занятия лекционного типа составляют 50% от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

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.

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 экзамену, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

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

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК - 7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК – 4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК - 5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК - 6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

ПК – 7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК – 10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК – 13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК - 15	способностью 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

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

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

ОПК – 7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				
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.

<p>владеть: -навыками анализа информационной инфраструктуры, выявления угроз информационной безопасности объекта информатизации и продемонстрировать способность и готовность к выбору комплекса средств и обоснованию критериев эффективности функционирования систем защиты информации на предприятии</p>	<p>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</p>	<p>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.</p>	<p>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.</p>	<p>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</p>
--	--	---	---	--

ПК 4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

<p>знать: - принципы формирования общих и детализированных политик информационной безопасности</p>	<p>Обучающийся демонстрирует полное отсутствие или недостаточное знание принципов формирования общих и детализированных политик информационной безопасности</p>	<p>Обучающийся демонстрирует неполное соответствие знаний принципов формирования общих и детализированных политик информационной безопасности, испытываются значительные затруднения при применении знаний в новых ситуациях</p>	<p>Обучающийся демонстрирует частичное соответствие знаний принципов формирования общих и детализированных политик информационной безопасности, но допускает незначительные ошибки, неточности, затруднения при аналитических ситуациях</p>	<p>Обучающийся демонстрирует полное соответствие знаний принципов формирования общих и детализированных политик информационной безопасности, и свободно оперирует приобретенными знаниями</p>
---	---	--	---	---

ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

<p>Владеть: - методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности</p>	<p>Обучающийся не владеет или в недостаточной степени владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности</p>	<p>Обучающийся владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности в неполном объеме, допускаются значительные ошибки, испытывает значительные затрудне-</p>	<p>Обучающийся частично владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности, навыки освоены, но допускаются незначительные ошибки, затруднения при переносе умений на</p>	<p>Обучающийся в полном объеме владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности свободно применяет полученные навыки в ситуациях повышенной сложности</p>
--	---	--	---	--

		ния при применении навыков в новых ситуациях.	новые, нестандартные ситуации.	
ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				
<p>уметь:</p> <ul style="list-style-type: none"> - 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 проведению 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 приобретенными умениями, применяет их в ситуациях повышенной сложности.
ПК – 7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
<p>уметь:</p> <ul style="list-style-type: none"> - 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 приобретенными умениями, применяет их в ситуациях повышенной сложности
ПК - 10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				

<p>знать: - существующие стандарты и методологии по управлению информационной безопасностью,</p>	<p>Обучающийся демонстрирует полное отсутствие или недостаточное знание существующих стандартов и методологии по управлению информационной безопасностью,</p>	<p>Обучающийся демонстрирует неполное знание существующих стандартов и методологии по управлению информационной безопасностью, испытываются значительные затруднения при применении навыков в новых ситуациях</p>	<p>Обучающийся демонстрирует частичное знание стандартов и методологии по управлению информационной безопасностью, но допускает значительные ошибки, неточности, затруднения при аналитических ситуациях</p>	<p>Обучающийся демонстрирует полное соответствие знаний стандартов и методологии по управлению информационной безопасностью, и свободно оперирует приобретенными знаниями.</p>
<p>уметь: - анализировать текущее состояние защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности;</p>	<p>Обучающийся не умеет или в недостаточной степени умеет анализировать текущее состояние защиты информации на предприятии с целью определения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности</p>	<p>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</p>	<p>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,</p>	<p>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</p>

ПК - 13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

<p>Уметь: - контролировать эффективность принятых мер по реализации политик безопасности</p>	<p>Обучающийся не умеет или в недостаточной степени умеет контролировать эффективность принятых мер по реализации политик безопасности</p>	<p>Обучающийся демонстрирует неполное умение в осуществлении контроля эффективности принятых мер по реализации политик безопасности, допускаются значительные ошибки, испытываются значительные затруднения при применении навыков в новых ситуациях</p>	<p>Обучающийся демонстрирует частичное умение в осуществлении контроля эффективности принятых мер по реализации политик безопасности, навыки освоены, но допускаются значительные ошибки, затруднения при переносе умений на новые, нестандартные ситуации.</p>	<p>Обучающийся демонстрирует полное умение в осуществлении контроля эффективности принятых мер по реализации политик безопасности, свободно применяет полученные навыки в ситуациях повышенной сложности</p>
---	--	--	---	--

ПК - 15 способностью 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

<p>знать: - нормативные правовые акты и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>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</p>	<p>Обучающийся демонстрирует неполное знание существующих нормативных правовых актов и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>Обучающийся демонстрирует частичное знание, нормативных правовых 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</p>	<p>Обучающийся демонстрирует полное соответствие знаний нормативных правовых актов и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю и свободно оперирует приобретенными знаниями.</p>
<p>уметь: -разрабатывать политики организации безопасности доступа к информации ограниченного пользования</p>	<p>Обучающийся не умеет или в недостаточной степени умеет разрабатывать политики организации безопасности доступа к информации ограниченного пользования и контролировать их применение</p>	<p>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</p>	<p>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.</p>	<p>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.</p>

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).

<i>Шкала оценивания</i>	<i>Описание</i>
<i>Отлично</i>	<i>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.</i>
<i>Хорошо</i>	<i>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.</i>
<i>Удовлетворительно</i>	<i>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.</i>
<i>Неудовлетворительно</i>	<i>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.</i>

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) 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. 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.)
3. Курс экономической теории. Учебник/Под ред. М.Н. Чепурина, Е.А. Киселевой. Киров, 2012. -752 с.
4. Мельников В.В. Государственное регулирование национальной экономики. Учебное пособие. М.: Омега-Л, 2012. -120 с.

б) дополнительная литература:

1. Астахов А.М. Искусство управления информационными рисками –М.: ДМК Пресс, 2010. (10 экз.)
2. Конев А.А., Давыдова Е.М., Шелупанов А.А. Управление информационной безопасностью: лабораторный практикум. – Томск: В-Спектр, 2017.

3. Ларина И.Е. Экономика защиты информации. Учебное пособие.; МГИУ, 2007 г – 96 с
4. Нестеров С.А. Основы информационной безопасности: Учебное пособие:- СПб.: [Издательство Политехнического университета](http://biblioclub.ru), 2014г. Режим доступа: <http://biblioclub.ru>

в) программное обеспечение и интернет-ресурсы:

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. STAFFCorp DLP-система (Пилотный проект)
4. Журнал «информационная безопасность» Режим доступа :<http://itsec.ru/imag/>

Полезные учебно-методические и информационные материалы представлены на сайтах:

1. Сайт Микрософт <https://www.microsoft.com/ru-ru/>
2. Сайт «Консультант Плюс» [www//consultant/ru](http://www.consultant.ru)

8. Материально-техническое обеспечение дисциплины.

Проведение лекционных и практических осуществляется в мультимедийной аудитории.

9. Методические рекомендации для самостоятельной работы студентов

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 задания, 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.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

Программу составил: к.э.н. доц.

Ларина И.Е.

Программа утверждена на заседании кафедры «Информационная безопасность»
«29» августа 2020 г., протокол № 1
Заведующий кафедрой



«Информационная безопасность» к.т.н., доцент
Федоров

Н.В.

**Структура и содержание дисциплины «Основы управления информационной безопасностью»
по направлению подготовки
10.03.01 «Информационная безопасность»
(бакалавр)**

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	РГР	Реферат	К/р	Э	З
	Первый семестр														
1.1	Основные задачи менеджмента в сфере информационной безопасности.	7	1-2	4			2								
1.2	<i>Лабораторная работа 1: Построение модели потенциального нарушителя ИС выбранного предприятия Задание на реферат</i>	7	1-2			4	4					+			
1.3	Роль международных организаций в сфере информационной безопасности	7	3-5	6			4								
1.4	<i>Лабораторная работа 2: Анализ защищенности объекта защиты информации Презентация рефератов</i>	7	3-4			4	4								
1.5	<i>Лабораторная работа 3: Подбор и обоснование выбора программ-</i>	7	5			2	4								

	<i>но-аппаратных средств авторизации доступа к информационным ресурсам предприятия.</i>													
1.6	Структура государственной системы защиты информации в РФ	7	6-8	6			4							
1.7	<i>Лабораторная работа 4 Основопологающие документы, определяющие политику РФ в сфере информационной безопасности</i>	7	6-7			4	2							
1.8	<i>Лабораторная работа 5 Структура государственной системы защиты информации и функции, выполняемые организациями государственной системы защиты информации</i> Контрольная работа	7	8			2	4						+	
1.9	Управление рисками информационной безопасности	7	9-10	4			4							
1.10	<i>Лабораторная работа 6 Методика управления рисками Майкрософт Презентация рефератов</i>	5	9-10			4	4						+	
1.11	Менеджмента в сфере информационной безопасности на уровне предприятий	7	11 - 13	6			4							
1.12	<i>Лабораторная работа 7 Разработка политики безопасности среднего и нижнего уровней</i>	7	11			2	4							

1.13	Лабораторная работа 8 <i>Обеспечение защиты информации при работе с кадрами.</i>	7	12			2	4								
1.14	Лабораторная работа 9 <i>Формирование плана мероприятий по повышению квалификации персонала департамента ИБ на период. Контрольная работа</i>	7	13			2	4						+		
1.15	Организация реагирования на чрезвычайные ситуации (инциденты)	7	14-16	6			4								
1.16	Лабораторная работа 10 Управление инцидентами ИБ. <i>Презентация рефератов</i>	7	14-15			4	4						+		
1.17	Аудит состояния информационной безопасности предприятия.	7	17-18	4			4								
1.18	<i>Представление и защита творческого задания</i> <i>Презентация рефератов</i>	7	16			2	4						+		
1.19	Лабораторная работа 11 Аудит ИБ <i>Презентация рефератов</i>	7	17			2	2						+		
1.20	<i>Итоговое практическое занятие</i>	7	18			2	2								
	Форма аттестации														Э
	Всего часов по дисциплине В семестре	144		36		36	72						Один	Две	

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

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем»

Форма обучения: очная

Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Основы управления информационной безопасностью»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Тестирование

Реферат

Контрольная работа

Творческое задание

Экзамен

Составители: к.э.н., доцент Ларина И.Е.

Москва, 2020 год

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Основы управления информационной безопасностью					
ФГОС ВО 10.03.01 «Информационная безопасность»					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие общепрофессиональные и профессиональные компетенции:					
КОМПЕТЕНЦИИ		Перечень компонентов	Технология формирования компетенций	Форма оценочного средства	Степени уровней освоения компетенций
ИН-ДЕКС	ФОРМУЛИРОВКА				
ОПК - 7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей	<p>знать:</p> <p>- основные угрозы безопасности и модели нарушителя информационной безопасности;</p> <p>владеть:</p> <p>- навыками анализа информационной инфраструктуры, выявления угроз информационной безопасности объекта информатизации и демонстрировать способность и готовность к выбору комплекса</p>	лекция, самостоятельная работа, лабораторные работы	ТЗ Т, Р	<p>Базовый уровень</p> <p>- способен определять основные угрозы безопасности и модели нарушителя информационной безопасности, владеть навыками анализа информационной инфраструктуры</p> <p>Повышенный уровень</p> <p>- способен формировать модель угроз и нарушителя, оценивать уровень защищенности объекта информатизации с целью определения целесообразности внедрения комплекса мер, правил, процедур, практических приемов, методов и средств обеспечения информационной безопасности</p>
ПК - 4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информацион-	<p>знать:</p> <p>- принципы формирования общих и детализированных политик информационной безопасности</p>	лекция, самостоятельная работа, лабораторные работы	ТЗ, К/Р, Т,	<p>Базовый уровень</p> <p>- способен, разрабатывать регламенты и должностные инструкции работников предприятия</p> <p>Повышенный уровень</p> <p>- способен разрабатывать политики безопасности среднего и нижнего уровней и контролировать их выполнение</p>

ПК – 5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	владеть: - методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности	лекция, самостоятельная работа	ТЗ, К/Р, Т, Р	Базовый уровень - способен принимать участие в проведении аттестации объектов информатизации на соответствие требованиям безопасности Повышенный уровень - владеет методикой проведения аттестации объектов информатизации на соответствие требованиям информационной безопасности и способен участвовать в сопровождении ее проведения
ПК – 6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных,	уметь: - оценивать информационные риски, проводить внутренний аудит состояния, работоспособности и эффективности применяемых средств и методов защиты информации.	лекция, самостоятельная работа, лабораторные работы	ТЗ, Т, Р	Базовый уровень - способен анализировать информационные риски и оценивать эффективность используемых методов защиты информации на предприятии. Повышенный уровень - способен оценивать информационные риски и проводить внутренний аудит состояния информационной безопасности на соответствие ее политикам безопасности предприятия.
ПК – 7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении	уметь: - составлять аналитические обзоры, разрабатывать предложения по совершенствованию системы управления информационной безопасностью на предприятии	лекция, самостоятельная работа, лабораторные работы	ТЗ, Т, Р	Базовый уровень - способен систематизировать научно-техническую и нормативную информацию и составлять аналитические обзоры Повышенный уровень - способен составлять аналитические обзоры, систематизировать научно-техническую и нормативную информацию, разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия.

ПК - 10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	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	лекция, самостоятельная работа, лабораторные работы	ТЗ, Т, К/Р Р	Базовый уровень - знает и может применять их на практике существующие стандарты управления информационной безопасностью, Повышенный уровень - знает методологии управления информационной безопасностью, владеет навыками анализа информационной инфраструктуры, и демонстрирует способность и готовность к выбору комплекса средств и обоснованию критериев эффективности функционирования систем защиты информации на предприятии.
ПК - 13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информации	уметь: - контролировать эффективность принятых мер по реализации политик безопасности	лекция, самостоятельная работа, лабораторные работы	ТЗ, Т, Р	Базовый уровень - способен контролировать эффективность принятых мер по реализации политик безопасности Повышенный уровень - способен контролировать и оценивать эффективность применяемых средств и методов защиты информации и вносить предложения по их совершенствованию
ПК - 15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности	знать: - нормативные правовые акты и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю уметь: - разрабатывать политики организации безопасного доступа к информации ограниченного пользования	лекция, самостоятельная работа, лабораторные работы	ТЗ, Т, Р	Базовый уровень - способностью, руководствуясь нормативно-правовыми актами и методическими документами, контролировать технологический процесс защиты информации ограниченного доступа Повышенный уровень способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы

1. Примерные темы рефератов, по курсу «Основы управления информационной 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 обеспечения безопасности. Менеджмент рисков безопасности
6. Менеджмент непрерывности бизнеса
7. Менеджмент оказания 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 её 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 происшествя;
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. специализированная 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 Р 51275)
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