

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования



**Пермский национальный исследовательский
политехнический университет**

УТВЕРЖДАЮ

Проректор по образовательной
деятельности

 А.Б. Петроченков

« 29 » мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Управление информационной безопасностью
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: магистратура
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 180 (5)
(часы (ЗЕ))

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления)

Направленность: Комплексные системы информационной безопасности
(наименование образовательной программы)

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

Задачи дисциплины:

- привитие обучаемым основ культуры обеспечения информационной безопасности;
- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем;
- обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.

1.2. Изучаемые объекты дисциплины

Понятия, методологии и практические приемы управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии и в организации

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-3	ИД-1ОПК-3	Знает отечественные и зарубежные стандарты в области управления информационной безопасностью.	Знает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов.	Отчет по практике

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-3	ИД-2ОПК-3	Умеет проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем управления информационной безопасностью.	Умет проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности.	Защита лабораторной работы
ОПК-3	ИД-3ОПК-3	Владеет навыками оценки и обработки рисков информационной безопасности, навыками разработки положения о применимости механизмов контроля состояния информационной безопасности в контексте управления рисками информационной безопасности	Владеет навыками навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности	Защита лабораторной работы
ОПК-5	ИД-1ОПК-5	Знает теоретические и эмпирические методы научных исследований, применяемые при управлении информационной безопасностью.	Знает теоретические и эмпирические методы научных исследований.	Отчёт по практическому занятию
ОПК-5	ИД-2ОПК-5	Умеет применять методы научных исследований в ходе решения задач по управлению информационной безопасностью.	Умеет применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей.	Защита лабораторной работы
ОПК-5	ИД-3ОПК-5	Владеет теоретическими и эмпирическими методами исследования процессов управления информационной безопасностью при выполнении работ по защите информации.	Владеет теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ.	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		3	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	54	54	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	18	18	
- лабораторные работы (ЛР)	16	16	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	18	18	
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	90	90	
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)	18	18	
Общая трудоемкость дисциплины	180	180	

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
3-й семестр				
Введение в дисциплину «Управление информационной безопасностью»	2	0	2	10
Цель и задачи изучения дисциплины. Базовая терминология. Система и системный подход. Процесс и процессный подход. Сущность и функции управления. Циклическая модель улучшения процессов. Понятие системы управления. Принципы управления. Цели и задачи управления информационной безопасностью.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Стандартизация систем и процессов управления информационной безопасностью	2	0	2	10
История развития стандартизации в области ИБ. Основные стандарты и методологии по управлению информационной безопасностью. Серия стандартов ISO 27000. Стандарты банковской системы Российской Федерации СТО БР ИББС. Рекомендации в области стандартизации. Стандарты на отдельные процессы управления информационной безопасностью и оценку безопасности информационных технологий: ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 18045, BS 25999/25777, ГОСТ Р 53647. Стандарты CoBiT. Преимущества и недостатки применения основных стандартов в области информационной безопасности.				
Управление и система управления информационной безопасностью	2	2	2	10
Деятельность по обеспечению информационной безопасностью организации. Основные методы управления информационной безопасностью. Управление информационной безопасностью информационно-телекоммуникационными технологиями организации. Система управления информационной безопасностью организации (СУИБ). Процессный подход в рамках управления информационной безопасностью организации. Работа с процессами СУИБ организацией. Стратегии построения и внедрения процессов СУИБ организацией. Совершенствование СУИБ				
Политика информационной безопасности.	2	2	2	10
Понятие политики информационной безопасности. Цели, требования и принципы при разработке и внедрении политики информационной безопасности. Порядок разработки частной политики информационной безопасности. Содержание и жизненный цикл политики информационной безопасности. Ответственность за исполнение политики информационной безопасности				
Оценка и обработка рисков информационной безопасности	2	2	2	10
Нормативное обеспечение управления рисками информационной безопасности. Основы рисковей деятельности. Сущность и роль управления рисками информационной безопасности. Порядок оценки рисков информационной безопасности. Методы оценки рисков информационной безопасности. Процесс обработки рисков как этап управления рисками информационной				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
безопасности. Варианты обработки рисков. Принятие, коммуникация, мониторинг и пересмотр рисков информационной безопасности. Обеспечение управления рисками информационной безопасности				
Управление инцидентами информационной безопасности	2	2	2	10
Нормативная база управления инцидентами информационной безопасности. Сущность процесса управления инцидентами информационной безопасности. Система управления инцидентами информационной безопасности. Этапы процесса управления инцидентами информационной безопасности				
Сущность аудита информационной безопасности	2	4	2	10
Назначение и цели аудита информационной безопасности. Виды аудита. Принципы проведения аудита информационной безопасности. Управление программой аудита информационной безопасности. Требования к аудитору информационной безопасности и оценка его работы. Измерение эффективности СУИБ. Метрики эффективности. Этапы и организация работ по проведению аудита информационной безопасности. Области и критерии аудита информационной безопасности. Анализ документации. Интервьюирование персонала и непосредственное наблюдение за деятельностью. Подготовку и утверждение отчета по аудиту информационной безопасности. Разработка мероприятий и проработка решений по устранению выявленных нарушений				
Технические аспекты управления информационной безопасностью	2	2	2	10
Политика в отношении логического доступа. Управление доступом пользователей. Обязанности пользователя при доступе к активам. Управление сетевым доступом. Управление доступом к операционной системе. Управление доступом к приложениям. Работа с мобильными устройствами в дистанционном режиме. Доступ к средствам обработки информации сторонних лиц и/или организаций.				
Технические аспекты управления информационной безопасностью	2	2	2	10
Защита от вредоносного программного обеспечения. Управление сетевыми ресурсами. Защита носителей информации. Обмен информацией и программного обеспечения. Вспомогательные операции. Выработка				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
требований по обеспечению информационной безопасности систем. Информационная безопасность приложений, исходных текстов программного обеспечения, исполняемых и системных файлов. Информационная безопасность данных и учетных записей. Информационная безопасность в процессах разработки и сопровождения информационных систем. Защитные меры, связанные с использованием криптографии. Управление конфигурациями, изменениями и обновлениями				
ИТОГО по 3-му семестру	18	16	18	90
ИТОГО по дисциплине	18	16	18	90

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Сущность и функции управления информационной безопасностью (СЗ)
2	Основные стандарты по управлению информационной безопасностью (СЗ)
3	Система управления информационной безопасностью (СЗ)
4	Разработка модели системы управления информационной безопасностью (СУИБ) предприятия (организации) (ПЗ)
5	Оценка рисков информационной безопасности (ПЗ)
6	Обработка рисков информационной безопасности (ПЗ)
7	Управление инцидентами информационной безопасности (ПЗ)
8	Назначение, цели и виды аудита информационной безопасности (СЗ)
9	Технические аспекты управления информационной безопасностью (ПЗ)

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Выбор области действия системы управления информационной безопасностью
2	Разработка политики информационной безопасности предприятия (организации)
3	Разработка частной политики управления рисками информационной безопасности
4	Разработка частной политики управления инцидентами информационной безопасности
5	Организация и проведение аудита информационной безопасности
6	Разработка частной политики управления логическим доступом

№ п.п.	Наименование темы лабораторной работы
7	Разработка частной политики защиты от вредоносного программного обеспечения

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Разработка системы управления информационной безопасностью предприятия (организации)

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

<p>Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.</p> <p>Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и принятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.</p> <p>Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.</p> <p>При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.</p>
--

5.2. Методические указания для обучающихся по изучению дисциплины

<p>При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу. 4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Милославская Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью : учебное пособие для вузов / Н. Г. Милославская, А. И. Толстой, М. Ю. Сенаторов. - Москва: Горячая линия-Телеком, 2018.	11
2	Милославская Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2012.	5
3	Милославская Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014.	5
4	Милославская Н. Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014.	15
5	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.]. - Москва: Горячая линия-Телеком, 2014.	15
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Анисимов А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2010.	2
2	Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. - Санкт-Петербург: БХВ-Петербург, 2003.	3
3	Северин В.А. Правовая защита информации в коммерческих организациях : учебное пособие для вузов / В.А. Северин. - Москва: Академия, 2009.	4
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-систем	http://vestnik.pstu.ru/get/_res/fs/file.pdf/5874/%D8%E0%E1%F3%F0%EE%E2+%C0.%D1.%2C+%C1%EE%F0%E8%F1%EE%E2+%C2.%C8.+%D0%E0%E7%F0%E0%E1%EE%F2%EA%E0+%EC%EE%E4%E5%EB%E8+%E7%E0%F9%E8%F2%FB+%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8+%EA%EE%F0%EF%EE%F0%E0%F2%E8%E2%ED%EE%E9+%	сеть Интернет; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Электронно-библиотечная система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	Персональный компьютер	10
Лабораторная работа	Персональный компьютер	10
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«Пермский национальный исследовательский политехнический
университет»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**для проведения промежуточной аттестации обучающихся по дисциплине
«Управление информационной безопасностью»
Приложение к рабочей программе дисциплины**

Направление подготовки: 10.04.01 Информационная безопасность

**Направленность (профиль)
образовательной программы:** Комплексные системы информационной
безопасности

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 2

Семестр: 3

Трудоёмкость:

Кредитов по рабочему учебному плану: 5 ЗЕ

Часов по рабочему учебному плану: 180 ч.

Форма промежуточной аттестации:

Экзамен: 3 семестр

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД освоение учебного материала дисциплины запланировано в течение одного семестра (4-го семестра учебного плана) и разбито на 2 учебных модуля. В каждом модуле предусмотрены аудиторские лекционные, практические и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, усвоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля					
	Текущий		Рубежный		Итоговый	
	С	ТО	ОЛР	Т/КР		Экзамен
Усвоенные знания						
З.1 Знает отечественные и зарубежные стандарты в области управления информационной безопасностью		ТО1				КЗ
З.2 Знает теоретические и эмпирические методы научных исследований, применяемые при управлении информационной безопасностью		ТО2				КЗ
Освоенные умения						
У.1 Умеет проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем управления информационной безопасностью.			ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР		
У.2 Умеет определять меры (правила, процедуры, применять методы научных исследований в ходе решения задач по управлению информационной безопасностью			ОЛР1 ОЛР2 ОЛР3 ОЛР4	КР		
Приобретенные владения						
В.1 Владеет и оценки и обработки рисков информационной безопасности, навыками разработки положения о применимости механизмов контроля состояния информационной безопасности в контексте управления рисками информационной безопасности.			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ

В.2 Владеет навыками теоретическими и эмпирическими методами исследования процессов управления информационной безопасностью при выполнении работ по защите информации			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
--	--	--	------------------------------	--	--	----

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учётом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, усвоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 4 лабораторных работы. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

Тема курсовой работы приведена в РПД. Курсовая работа содержит комплексное практическое задание – разработать систему управления информационной безопасностью предприятия (организации).

Защита курсовой работы проводится индивидуально каждым студентом путем собеседования по расчетной части и демонстрации результатов разработки программной модели. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки усвоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности *всех* заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Взаимосвязь понятий «управление» «процесс» и «система». Сущность системного подхода.
2. Понятие системы управления и его структура. Сущность и функции управления.
3. Принципы управления и их сущность.
4. Цель и задачи управления информационной безопасностью (ИБ).
5. Основные сведения об ISO. Этапы развития стандартов ISO 27001 и 27002.
6. Преимущества и недостатки внедрения системы управления ИБ в соответствии со стандартами ISO.
7. Основные национальные стандарты РФ по управлению ИБ.

8. Преимущества внедрения системы управления ИБ на основе стандарта ISO 27001 для предприятия.
9. Отраслевые стандарты СТО БР ИББС РФ.
10. Рекомендации по стандартизации серии СТО БР ИББС РФ.
11. Стандарты CoViT. Показатели эффективности CoViT.
12. Стандарты ISO 18044 ISO 18045 (ГОСТ Р ИСО/МЭК ТО 18044/18045).
13. Понятие, структура и категории политик ИБ.
14. Цель, основные задачи и причины разработки и внедрения политики ИБ предприятия (организации).
15. Требования и принципы при разработке и внедрении политики ИБ предприятия (организации).
16. Содержание и жизненный цикл политики ИБ предприятия (организации).
17. Управление ИБ предприятия (организации). Цели процесса управления в соответствии с SLA.
18. Уровни процесса управления ИБ предприятия (организации).
19. Процессный подход для управления ИБ и его составляющие.
20. Система управления информационной безопасностью (СУИБ) организации и цель ее разработки. Требования к СУИБ.
21. Процессный подход управления ИБ. Цикл PDCA и его компоненты.
22. Характеристика этапов создания СУИБ и их логическая взаимосвязь.
23. Содержание документации для создания СУИБ предприятия (организации).
24. Система сертификации ISO. Преимущества сертификации СУИБ для предприятия (организации).
25. Основы рисковей деятельности: понятие риска, актива, уязвимости. Нормативное обеспечение управления рисками ИБ. Зона возможного риска ИБ.
26. Управление рисками (риск-менеджмент). Этапы и задачи управления рисками.
27. Управление рисками ИБ. Подходы к управлению рисками ИБ.
28. Содержание процесса управления рисками ИБ. Соответствие цикла СУИБ и PDCA.
29. Содержание деятельности по оценке рисков ИБ. Этапы анализа и оценивания рисков ИБ.
30. Содержание процесса обработки рисков ИБ.
31. Варианты обработки рисков ИБ (снижение, сохранение, избежание, передача риска).
32. Принятие, коммуникация, мониторинг и пересмотр рисков ИБ.
33. Документальное обеспечение управления рисками ИБ.
34. Инструментальные средства управления рисками ИБ.
35. Событие и инцидент. Реализации преднамеренного инцидента ИБ.
36. Управление инцидентами ИБ. Цели организации по управлению инцидентами ИБ.
37. Этапы процесса управления инцидентами ИБ, в соответствии с моделью PDCA.
38. Содержание порядка действий в случае инцидентов ИБ.
39. Применение SOC-центров для управления инцидентами ИБ.
40. Техническая, документационная и организационная поддержка системы управления инцидентами ИБ.

41. Виды проверок СУИБ. Мониторинг и самооценка ИБ.
42. Понятие, нормативное обеспечение, цели и виды аудита ИБ. Принципы проведения аудита.
43. Программа аудита ИБ. Управление программой аудита ИБ.
44. Требования к аудитору ИБ и оценка его работы.
45. Измерение эффективности СУИБ. Метрики эффективности.
46. Содержание и организация процесса аудита ИБ.
47. Отчетные документы по результатам проведения аудита ИБ.
48. Управление и политика ИБ в отношении логического доступа. Общие правила управления доступом.
49. Управление доступом пользователей. Регистрация и отмена регистрации пользователей для предоставления и отмены доступа. Привилегии. Пересмотр прав доступа.
50. Управление доступом к операционной системе.
51. Управление доступом к приложениям.
52. Управление работой с мобильными устройствами в дистанционном режиме.
53. Управление сетевым доступом. Методы управления защитой больших сетей.
54. Организационные основы безопасной операционной деятельности.
55. Доступ к средствам обработки информации.
56. Планирование нагрузки и приемка систем.
57. Защита от вредоносных программ и безопасность носителей информации.
58. Управление сетевыми ресурсами.
59. Обмен информацией, программным обеспечением и вспомогательные операции.
60. Политика применения средств криптографической защиты информации (СКЗИ).

Типовые вопросы и практические задания для контроля освоенных умений:

1. Осуществить разработку модели СУИБ в составе требуемых компонентов.
2. Разработать алгоритм Процесса управления рисками информационной безопасностью на основании реализации модели PDCA.
3. Провести обработку рисков информационной безопасности на основании анализа и оценки рисков информационной безопасности и в соответствии с выбранной областью действия СУИБ и активами.
4. Сформировать требования по организации процесса мониторинга, коммуникации и пересмотра рисков ИБ.
5. Сформировать основные положения Политики управления инцидентами информационной безопасности для предприятия (организации).
6. Разработать политику управления доступом к активам организации (предприятия),
7. Разработать частную политику управления защищенной передачей данных организации (предприятия).

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины.*

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.