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: Основы защиты информации
(наименование)

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

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

Общая трудоёмкость: 72 (2)
(часы (ЗЕ))

Направление подготовки: 27.04.04 Управление в технических системах
(код и наименование направления)

Направленность: Распределенные компьютерные информационно-управляющие системы
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - изучение принципов обеспечения информационной безопасности и защиты информации, подходов к анализу угроз безопасности информационных систем и освоение компетенций для решения основных задач защиты информации в информационных системах

Задачи дисциплины:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации;
- приобретение навыков анализа информационной инфраструктуры с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

1.2. Изучаемые объекты дисциплины

- основные понятия, общеметодологические принципы теории информационной безопасности;
- основы государственной информационной политики по обеспечению безопасности информации;
- виды информации ограниченного доступа;
- угрозы безопасности информации и уязвимости информационных систем;
- информационные войны и информационное оружие;
- методы нарушения конфиденциальности, целостности и доступности информации;
- причины, виды каналы утечки информации и несанкционированного доступа;
- формальные модели безопасности информации;
- уровни и сервисы защиты информации;
- способы и средства защиты информации;
- критерии оценки защищенности информационных систем;
- основы организации защиты информации на предприятии.

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

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
УК-1	ИД-1УК-1.	Способен осуществлять критический анализ проблемных ситуаций в области обеспечения личной и корпоративной информационной безопасности, принимать необходимые решения по защите информации.	Знает методы критического анализа и оценки современных научных достижений; основные принципы критического анализа.	Отчёт по практическому занятию
УК-1	ИД-2УК-1.	Умеет получать новые знания собирать данные по проблемам обеспечения информационной безопасности, участвовать в решении задач по защите информации в профессиональной деятельности.	Умеет получать новые знания на основе анализа, синтеза и др.; собирать данные по сложным научным проблемам, относящимся к профессио-нальной области; осуществлять поиск информации и решений на основе дей-ствий, эксперимента и опыта.	Отчёт по практическому занятию
УК-1	ИД-3УК-1.	Владеет навыками оценки ситуаций и проблем в области защиты информации, основными действиями по их решению в личной и профессиональной сфере.	Владеет навыками исследования проблемы профессиональной деятельности с применением анализа; синтеза и других методов интеллекту-альной деятельности; навыками выяв-ления научных проблем и использова-ния адекватных методов для их реше-ния; навыками оценочных суждений при решении проблемных профессио-нальных ситуаций.	Отчёт по практическому занятию

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: 1.1. Контактная аудиторная работа, из них:	29	29
- лекции (Л)	9	9
- лабораторные работы (ЛР)		
- 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)	43	43
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет		
Зачет	9	9
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	72	72

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				
Основные понятия и общеметодологические принципы теории информационной безопасности	2	0	2	4
Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Основы государственной политики в информационной сфере	0	0	2	5
Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.				
Понятие и виды защищаемой информации	2	0	2	5
Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.				
Понятие и виды угроз безопасности информации	2	0	2	4
Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информа-ционной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации.				
Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны	0	0	2	5
Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационной войны.				
Методы и средства обеспечения информационной безопасности	2	0	2	5

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.				
Механизмы и сервисы защиты информации	0	0	2	5
Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.				
Формальные модели безопасности информационных систем	1	0	2	5
Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-Ла-Падулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.				
Методы и критерии оценки защищенности компьютерных систем	0	0	2	5
Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. Руководящие документы ФСТЭК России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.				
ИТОГО по 3-му семестру	9	0	18	43
ИТОГО по дисциплине	9	0	18	43

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Основные понятия и общеметодологические принципы теории информационной безопасности
2	Основы государственной политики и угрозы безопасности информации в информационной сфере
3	Определение вида и состава информации ограниченного доступа
4	Классификация угроз безопасности информации
5	Основы информационного противоборства и применения информационного оружия
6	Применение способов и средств защиты информации
7	Основные сервисы защиты информации в информационных системах. Защищенные протоколы информационного взаимодействия
8	Формальные модели обеспечения безопасности информации
9	Критерии оценки защищенности инормационных и автоматизированных систем

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

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.

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 приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

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	Данилов А. Н. Основы информационной безопасности : учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. - Пермь: Изд-во ПГТУ, 2008.	63
2	Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - Москва: Академия, 2009.	10
3	Цирлов В. Л. Основы информационной безопасности : краткий курс / В. Л. Цирлов. - Ростов-на-Дону: Феникс, 2008.	9
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Защита информации : учебное пособие для вузов / А. П. Жук [и др.]. - Москва: РИОР, ИНФРА-М, 2015.	5
2	Новиков В. К. Информационная безопасность и защита информации. Организационно-правовые основы / В. К. Новиков, И. Б. Галушкин. - Москва: Горячая линия-Телеком, 2018.	3
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	МОДЕЛЬ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	http://vestnik.pstu.ru/get/_res/fs/file.pdf/8281/%CC%CE%C4%C5%CB%DC+%CE%C1%CD%C0%D0%D3%C6%C5%CD%C8%DF+%CA%CE%CC%CF%DC%DE%D2%C5%D0%CD%DB%D5+%C0%D2%C0%CA++%CD%C0+%CE%C1%DA%C5%CA%D2%DB+%CA%D0%C8%D2%C8%D7%C5%D1%CA%CE%C9+%C8%CD%D4%CE%D0%CC%C0%D6%C8%CE%CD%CD%CE	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
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Электронно-библиотечная система ЮРАЙТ	https://biblio-online.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
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 «Основы защиты информации»
Приложение к рабочей программе дисциплины

Направление подготовки: 27.04.04 Управление в технических системах

Направленность (профиль) образовательной программы: Распределённые компьютерные информационно-управляющие системы

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 2 **Семестр**: 3

Трудоёмкость:
Кредитов по рабочему учебному плану: 2 ЗЕ
Часов по рабочему учебному плану: 72 ч.

Форма промежуточной аттестации:
Зачёт: 3 семестр

Пермь 2021

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 (3-го семестра учебного плана). Предусмотрены аудиторные лекционные и практические занятия. 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, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и зачета. 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**		**Зачёт**
Усвоенные знания						
З.1 знать методы критического анализа и оценки современных научных достижений; основные принципы критического анализа.	С			КР		ТВ
Освоенные умения						
У.1 получать новые знания на основе анализа, синтеза и др.; собирать данные по сложным научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и решений на основе действий, эксперимента и опыта.	С			КР		ПЗ
Приобретенные владения						
В.1 владеть навыками исследования проблемы профессиональной деятельности с применением анализа; синтеза и других методов интеллектуальной деятельности; навыками выявления научных проблем и использования адекватных методов для их решения; навыками оценочных суждений при решении проблемных профессиональных ситуаций.				ПЗ		ПЗ

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 дифференцированного зачета.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде зачета, 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, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме рубежного тестирования (после проведения практических занятий).

2.2.1. Рубежная контрольная работа

Всего запланировано 7 рубежных контрольные работы (КР) после освоения студентами учебных модулей дисциплины и проведения практических занятий.

Типовые задания КР:

1. Определение типа защищаемой информации, составление перечня защищаемых сведений.

2. Разработка модели нарушителя.

3. Разработка модели угроз.

4. Разработка модели нарушителя и угроз для для гос. организации.

5. Разработка политики защиты информации, выбор методов и средств защиты.

6. Разработка формальной модели безопасности информационной системы.

7. Разработка методики оценки угроз и состояния защищённости информационных ресурсов.

Типовые шкала и критерии оценки результатов рубежной контрольной работы 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 практических работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

2.3.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания

Промежуточная аттестация проводится в форме зачета. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде зачета приведены в общей части ФОС образовательной программы.

2.3.2. Процедура промежуточной аттестации с проведением аттестационного испытания

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций.

2.4.2.1. Типовые вопросы и задания для зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Основные понятия и общеметодологические принципы теории информационной безопасности.

2. Основы государственной политики в информационной сфере.

3. Понятие и виды защищаемой информации.

4. Понятие и виды угроз безопасности информации.

5. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.

6. Методы и средства обеспечения информационной безопасности.
7. Механизмы и сервисы защиты информации.
8. Формальные модели безопасности информационных систем.
9. Методы и критерии оценки защищенности компьютерных систем.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Определить тип защищаемой информации
2. Составить перечень защищаемых сведений.
3. 2. Разработать модель нарушителя.
4. Разработать модель угроз.
5. Разработать модель нарушителя и угроз для для гос. организации.
6. Разработать политику защиты информации.
7. Разработать формальную модель безопасности информационной системы.
8. Разработать методику оценки угроз.
9. Разработать методику состояния защищённости информационных ресурсов.

2.4.2.2. Шкалы оценивания результатов обучения на зачете

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

Типовые шкала и критерии оценки результатов обучения при сдаче зачета 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 зачете считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

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 зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.

Примеры вопросов для проверки знаний:

1. Состояние информации, при котором допуск к ней осуществляют лишь субъекты, которые имеют такое право
✓ Конфиденциальность
o Целостность
o Доступность

2. Избежание несанкционированных изменений информации
o Конфиденциальность
✓ Целостность
o Доступность

3. Избежание постоянного или временного сокрытия информации от субъектов, которые имеют права доступа
o Конфиденциальность
o Целостность
✓ Доступность

4. Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов
✓ Антивирус
o Межсетевой экран (брандмауэр)
o Система обнаружения вторжения

5. Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами
o Антивирус
✓ Межсетевой экран (брандмауэр)
o Система обнаружения вторжения

6. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
✓ Персональные данные
o Коммерческая тайна
o Государственная тайна

7. Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
o Персональные данные

- ✓ Коммерческая тайна
- o Государственная тайна

8. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государству
- o Персональные данные
- o Коммерческая тайна
- ✓ Государственная тайна