Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники
(Наименование института)

УТВЕРЖДАЮ:
Директор института
_____ А.А. Галкин
«20» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
(наименование дисциплины)

направление подготовки / специальность
10.04.01. «Информационная безопасность»

направленность (профиль) подготовки
Автоматизация информационно-аналитической деятельности

г. Владимир

2023 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Управление информационной безопасностью» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО 3++ и учебного плана по направлению 10.04.01 «Информационная безопасность». В процессе подготовки обеспечивается формирование у студентов обобщенного представления об основных принципах и возможностях обеспечения управления информационной безопасностью на объекте защиты.

В ходе освоения дисциплины проводится ознакомление студентов с механизмами создания системы управления информационной безопасностью, контроля за работой средств управления (СУИБ) на предприятии. Рассматривается мониторинг и оценка рисков управления информационной безопасностью.

Задачей дисциплины «Управление информационной безопасностью» является освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в автоматизированных информационных системах (АИС). В процессе освоения дисциплины изучаются следующие вопросы: основные руководящие документы и показатели эффективности системы защиты информации; комплексный подход к обеспечению ИБ; цели, стратегии и политика информационной безопасности; организационные аспекты информационной безопасности; функции управления информационной безопасностью; процессный подход для управления информационной безопасностью; система ответственности в области информационной безопасности; оценивание риска в информационных системах на основе объективных оценок для повышения достоверности при расчете экспертных оценок; объективная стоимостная оценка предсказания величины ущерба от нарушений безопасности ИР; оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации; оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности; концепция проведения менеджмента риска на предприятии; программные средства для проведения аудита информационной безопасности; концепция построения системы безопасности предприятия; особенности применения средств защиты для обеспечения безопасности системы электронного документооборота; правовые основы деятельности службы безопасности предприятия; методика проектирования организационной структуры службы безопасности; организация службы защиты информации; управление службой безопасности предприятия, работа с кадрами; требования к специалистам по защите информации; организация обучения специалистов по защите информации.

Задачей дисциплины также является овладение навыками практической деятельности в области моделирования и анализа технических средств управления информационной безопасностью в АИС и службой безопасности на предприятии с использованием средств вычислительной техники, умение использовать соответствующее специализированное программное обеспечение.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части Блока Б1 (код Б1.О.06). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, практических занятий и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора)*	Результаты обучения по дисциплине	
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1.1	Знать этапы жизненного цикла проекта, принципы формирования концепции проекта в рамках обозначенной проблемы, основные требования, предъявляемые к проектной работе и критерии оценки результатов проектной деятельности	КР Тестовые вопросы
	УК-2.2.1	Уметь разрабатывать концепцию проекта, формулируя цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа проекта), ожидаемые результаты и возможные сферы их применения	
	УК-2.3.1	Владеть навыками составления плана реализации проекта и контроля его выполнения	
УК-3 Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1.1	Знать методы управления и организации командной работы, основы стратегического планирования работы коллектива для достижения поставленной цели	КР Тестовые вопросы
	УК-3.2.1	Уметь разрабатывать командную стратегию, организовывать работу коллектива, разрабатывать мероприятия по личностному, образовательному и профессиональному росту	
	УК-3.3.1	Владеть навыками постановки цели в условиях командой работы, способами управления командной работой в решении поставленных задач, навыками преодоления возникающих в коллективе разногласий, споров и конфликтов на основе учета интересов всех сторон	
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1.1	Знать основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе	КР Тестовые вопросы
	ОПК-3.1.2	Знать основные угрозы безопасности информации и модели нарушителя в информационных системах	
	ОПК-3.1.3	Знать принципы формирования политики информационной безопасности в информационных системах	
	ОПК-3.1.4	Знать основы теории рисков информационной безопасности; основные модели, стандарты и нормативно-распорядительные документы государственных регуляторов по вопросам управления процессами обеспечения информационной безопасности	

	ОПК-3.1.5	Знать источники и классификация угроз информационной безопасности	
	ОПК-3.1.6	Знать методы аттестации уровня защищенности информационных систем	
	ОПК-3.1.7	Знать основные методы управления информационной безопасностью	
	ОПК-3.1.8	Знать основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем	
	ОПК-3.1.9	Знать принципы функционирования автоматизированных систем поддержки документооборота и их безопасности	
	ОПК-3.1.10	Знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	
	ОПК-3.2.1	Уметь создавать формальные модели управления процессами обеспечения информационной безопасности	
	ОПК-3.2.2	Уметь прогнозировать состояние информационной безопасности объекта защиты на основе использования теории рисков	
	ОПК-3.2.3	Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	
	ОПК-3.2.4	Уметь строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем	
	ОПК-3.2.5	Уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	
	ОПК-3.2.6	Уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем	
	ОПК-3.2.7	Уметь разрабатывать частные политики информационной безопасности информационных систем	
	ОПК-3.2.8	Уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем	
	ОПК-3.2.9	Уметь оценивать информационные риски в информационных системах	
	ОПК-3.2.10	Уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем	
	ОПК-3.2.11	Уметь составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем	
	ОПК-3.2.12	Уметь обосновывать принципы организации технического, программного и информационного обеспечения ИБ	

	ОПК-3.3.1	Владеть основными системными подходами к определению целей, задач обеспечения информационной безопасности в автоматизированных системах	
	ОПК-3.3.2	Владеть основными навыками поиска информации о современных и перспективных методах обеспечения информационной безопасности в автоматизированных системах и поиска источников специальной информации, необходимой в профессиональной деятельности	
	ОПК-3.3.3	Владеть навыками формирования комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в ИАС информации ограниченного доступа	
	ОПК-3.3.4	Владеть навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	
	ОПК-3.3.5	Владеть навыками организации процесса разработки частных политик безопасности компьютерных систем, в том числе политик управления доступом и информационными потоками	
	ОПК-3.3.6	Владеть методами управления информационной безопасностью информационных систем	
	ОПК-3.3.7	Владеть методами оценки информационных рисков	
	ОПК-3.3.8	Владеть методами организации и управления деятельностью служб защиты информации на предприятии	
	ОПК-3.3.9	Владеть навыками управления информационной безопасностью простых объектов	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 9 зачетных единицы, 324 часа

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	**Раздел 1.** Парадигма системы управления информационной безопасностью.	1	1	2	2			2	
2	**Раздел 2.** Процессный подход в управлении информационной безопасностью.	1	2	2	2			2	
3	**Раздел 4.** Оценивание риска в информационных системах на основе объективных оценок для повышения достоверности при расчете экспертных оценок.	1	3	2	2			2	
4	**Раздел 4.** Алгоритм расчета объективной вероятности реализаций неблагоприятных событий в компьютерной системе	1	4	2	2			2	
5	**Раздел 5.** Объективная стоимостная оценка предсказания величины ущерба от нарушений безопасности ИР.	1	5	2	2			2	
6	**Раздел 6.** Алгоритм фильтра Калмана. Случай взаимно-коррелированных шумов динамики и измерителя	1	6	2	2			2	Рейтинг-контроль №1
7	**Раздел 7.** Оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации.	1	7	2	2			2	
8	**Раздел 8.** Оптимальный выбор средств комплексной системы защиты информации от возможных угроз ИБ.	1	8	2	2			2	
9	**Раздел 9.** Оптимальный выбор средств комплексной системы защиты информации от возможных угроз ИБ. Методика решения задачи.	1	9	2	2			2	

10	**Раздел 10.** Методология менеджмента риска.	1	10	2	2			2	
11	**Раздел 11.** Концепция проведения менеджмента риска на предприятии.	1	11	2	2			2	
12	**Раздел 12.** Методика проведения аудита информационной безопасности на предприятии.	1	12	2	2			2	Рейтинг-контроль №2
13	**Раздел 13.** Организация и проведения работ по аудиту ИБ на предприятии.	1	13	2	2			2	
14	**Раздел 14.** Выработка рекомендаций и подготовка отчетных документов аудита ИБ на предприятии.	1	14	2	2			2	
15	**Раздел 15**. Программные средства для проведения аудита информационной безопасности	1	15	2	2			2	
16	**Раздел 16.** Программные средства для проведения аудита информационной безопасности. Система CRAMM.	1	16	2	2			2	
17	**Раздел 17.** Программные средства для проведения аудита информационной безопасности. Система КОНДОР.	1	17	2	2			2	
18	**Раздел 18.** Программные средства для проведения аудита информационной безопасности. Использование сетевых сканеров.	1	18	2	2			2	Рейтинг-контроль №3
Всего за 9 семестр:		**144**		**36**	**36**			**36**	**Экзамен (36)**
19	**Раздел 1.** Концепция построения системы безопасности предприятия.	2	1	2	2			4	
20	**Раздел 2.** Концептуальные модели компонентов системы безопасности предприятия.	2	2	2	2			4	
21	**Раздел 3.** Особенности применения средств защиты для обеспечения безопасности системы электронного документооборота (СЭД).	2	3	2	2			4	
22	**Раздел 4.** Контроль целостности объектов СЭД.	2	4	2	2			4	
23	**Раздел 5.** Защита данных в облачных системах работы с электронными документами СЭД.	2	5	2	2			4	
24	**Раздел 6.** Правовые основы деятельности службы безопасности предприятия.	2	6	2	2			4	Рейтинг-контроль №1

25	**Раздел 7.** Организационное проектирование деятельности службы безопасности предприятия.	2	7	2	2			4	
26	**Раздел 8.** Методика проектирования организационной структуры системы управления.	2	8	2	2			4	
27	**Раздел 9.** Структура и функции службы безопасности предприятия.	2	9	2	2			4	
28	**Раздел 10.** Построение структурной схемы управления службой безопасности предприятия.	2	10	2	2			4	
29	**Раздел 11.** Подразделения службы безопасности предприятия.	2	11	2	2			4	
30	**Раздел 12.** Организация службы защиты информации.	2	12	2	2			4	Рейтинг-контроль №2
31	**Раздел 13.** Организационно-технические мероприятия СЗИ.	2	13	2	2			4	
32	**Раздел 14.** Руководитель службы защиты информации, его права и обязанности.	2	14	2	2			4	
33	**Раздел 15.** Управление службой безопасности предприятия (СБП).	2	15	2	2			4	
34	**Раздел 16.** Обеспечение деятельности службы безопасности.	2	16	2	2			4	
35	**Раздел 17.** Подбор, расстановка и обучение сотрудников службы защиты информации.	2	17	2	2			4	
36	**Раздел 18.** Требования к специалистам по защите информации.	2	18	2	2			4	Рейтинг-контроль №3
Всего за семестр «А»:		**180**		**36**	**36**			**72**	**Экзамен (36)**
Наличие в дисциплине КП/КР		**ДА (2)**							
Итого по дисциплине		**324**		**72**	**72**			**108**	**Экзамен (36)** **Экзамен (36)** **Курсовая работа**

Содержание лекционных занятий по дисциплине

Семестр 1

Раздел 1. Парадигма системы управления информационной безопасностью. Роль информационной безопасности, как процесса. Цикл Шухарта–Деминга.

Раздел 2. Процессный подход в управлении информационной безопасностью. Документированность системы управления информационной безопасностью. Организационно-технические требования системы управления информационной безопасностью.

Раздел 4. Оценивание риска в информационных системах на основе объективных оценок для повышения достоверности при расчете экспертных оценок.
Раздел 4. Алгоритм расчета объективной вероятности реализаций неблагоприятных событий в компьютерной системе
Раздел 5. Объективная стоимостная оценка предсказания величины ущерба от нарушений безопасности ИР. Группы контролей безопасности
Раздел 6. Алгоритм фильтра Калмана. Случай взаимно-коррелированных шумов динамики и измерителя
Раздел 7. Оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации. Анализ защищенности информационных ресурсов предприятия.
Раздел 8. Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Постановка задачи.
Раздел 9. Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Методика решения задачи.
Раздел 10. Методология менеджмента риска. Основные понятия управления риском на предприятии. Принципы управления риском на предприятии.
Раздел 11. Концепция проведения менеджмента риска на предприятии. Процесс риск-менеджмента на предприятии.
Раздел 12. Методика проведения аудита информационной безопасности на предприятии. Три подхода к проведению аудита ИБ. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ. Планирование процедуры аудита ИБ.
Раздел 13. Организация и проведения работ по аудиту ИБ на предприятии. Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ на предприятии.
Раздел 14. Выработка рекомендаций и подготовка отчетных документов аудита ИБ на предприятии. Экономическая оценка обеспечения ИБ предприятия.
Раздел 15. Программные средства для проведения аудита информационной безопасности Сравнительный анализ видов используемых программных продуктов.
Раздел 16. Программные средства для проведения аудита информационной безопасности. Система CRAMM.
Раздел 17. Программные средства для проведения аудита информационной безопасности. Система КОНДОР.
Раздел 18. Программные средства для проведения аудита информационной безопасности. Использование сетевых сканеров.

Семестр 2
Раздел 1. Концепция построения системы безопасности предприятия. Защита информации в системе безопасности предприятия.
Раздел 2. Концептуальные модели компонентов системы безопасности предприятия. Принципы построения системы безопасности предприятия.
Раздел 3. Особенности применения средств защиты для обеспечения безопасности системы электронного документооборота (СЭД). Средства защиты информации. Управление доступом в защищенной СЭД.
Раздел 4. Контроль целостности объектов СЭД. Криптографические средства и методы защиты информации и персональных данных в СЭД. Межсетевое экранирование и антивирусная защита для обеспечения безопасности СЭД.
Раздел 5. Защита данных в облачных системах работы с электронными документами СЭД. Безопасность мобильных устройств, применяемых в СЭД. Защита данных на сетевом и транспортном уровне.
Раздел 6. Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы системы безопасности предприятия. Виды

нормативных документов. Лицензирование видов деятельности службы безопасности предприятия. Рекомендации по разработке уставных документов службы безопасности предприятия.

Раздел 7. Организационное проектирование деятельности службы безопасности предприятия. Основы организационного проектирования систем управления. Методика проектирования функционального содержания управленческой деятельности.

Раздел 8. Методика проектирования организационной структуры системы управления. Методика оформления основных документов организационного проекта системы управления.

Раздел 9. Структура и функции службы безопасности предприятия. Состав службы безопасности предприятия. Основные функции службы безопасности предприятия.

Раздел 10. Построение структурной схемы управления службой безопасности предприятия.

Раздел 11. Подразделения службы безопасности предприятия. Подразделения режима и охраны. Подразделение информационно-аналитической деятельности. Режимно-секретное подразделение. Подразделение инженерно-технической защиты.

Раздел 12. Организация службы защиты информации. Создание СЗИ. Структура СЗИ.

Раздел 13. Организационно-технические мероприятия СЗИ.

Раздел 14. Руководитель службы защиты информации, его права и обязанности. Методика разработки должностных инструкций для специалистов по защите информации.

Раздел 15. Управление службой безопасности предприятия (СБП). Методы управления СБП. Функции процессов управления СПБ. Принципы управления СБП.

Раздел 16. Обеспечение деятельности службы безопасности. Управление безопасностью предприятия в кризисных ситуациях.

Раздел 17. Подбор, расстановка и обучение сотрудников службы защиты информации. Роль персонала в системе защиты информации. Роль персонала в системе защиты информации. Набор и отбор персонала в СБП.

Раздел 18. Требования к специалистам по защите информации. Организация обучения специалистов по защите информации. Требования к начальнику службы безопасности предприятия. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия.

Содержание практических занятий по дисциплине

Темы практических занятий 1 семестр

Практическое занятие №1. Изучение параметров информационных систем и показателей качества систем защиты информации предприятия. Знакомство с возможностями программного комплекса Microsoft Security Assessment Tool (MSAT).

Практическое занятие №2. Организация и проведение экспертизы АИС предприятия. Методы экспертных оценок.

Практическое занятие №3. Организация и проведение экспертизы АИС предприятия. Нечеткие множества и нечеткие числа. Нечеткие меры.

Практическое занятие №4. Аудит степени соответствия параметров СЗИ требованиям стандартов безопасности.

Практическое занятие №5. Методика оценки показателей качества СЗИ предприятия.

Практическое занятие №6. Методика оценки угроз безопасности информации ФСТЭК России.

Практическое занятие №7. База данных угроз безопасности информации ФСТЭК России.

Практическое занятие №8. Расчет показателей качества системы защиты информации на примере коммерческого предприятия. Часть 1.

Практическое занятие №9. Расчет показателей качества системы защиты информации на примере коммерческого предприятия. Часть 2.

Темы практических занятий 2 семестр

Практическое занятие №1. Разработка положения о службе безопасности предприятия (Устав службы безопасности).

Практическое занятие №2. Разработка положения «О защите информации ограниченного доступа от ее утечки по техническим каналам».

Практическое занятие №3. Разработка положения «О подразделении инженерно-технической защиты информации».

Практическое занятие №4. Разработка положения «О подразделении охраны и режима».

Практическое занятие №5. Разработка инструкции «Об осуществлении контрольно-пропускного и объектового режима на объекте».

Практическое занятие №6. Разработка положения «О постоянно действующей экспертной комиссии по защите конфиденциальной информации».

Практическое занятие №7. Разработка инструкции (положения, руководства) по защите информации ограниченного доступа на объекте.

Практическое занятие №8. Разработка инструкции (положения, руководства) по защите информации ограниченного доступа при ее обработке с помощью средств вычислительной техники на объекте.

Практическое занятие №9. Разработка положения о введении режима коммерческой тайны на предприятии.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Семестр 1

Перечень вопросов к рейтинг-контролю №1

- Парадигма системы управления информационной безопасностью.
- Роль информационной безопасности, как процесса. Цикл Шухарта–Деминга.
- Процессный подход в управлении информационной безопасностью.
- Документированность системы управления информационной безопасностью.
- Организационно-технические требования системы управления информационной безопасностью.
- Оценивание риска в информационных системах на основе объективных оценок для повышения достоверности при расчете экспертных оценок.
- Алгоритм расчета объективной вероятности реализаций неблагоприятных событий в компьютерной системе
- Объективная стоимостная оценка предсказания величины ущерба от нарушений безопасности ИР. Группы контролей безопасности
- Использование алгоритма фильтра Калмана для оценки величины ущерба от нарушений безопасности ИР. Случай взаимно-коррелированных шумов динамики и измерителя
- Оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации.
- Анализ защищенности информационных ресурсов предприятия.
- Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Постановка задачи.

Перечень вопросов к рейтинг-контролю №2

- Оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации.

- Анализ защищенности информационных ресурсов предприятия.
- Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Постановка задачи.
- Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Методика решения задачи.
- Методология менеджмента риска. Основные понятия управления риском на предприятии. Принципы управления риском на предприятии.
- Концепция проведения менеджмента риска на предприятии. Процесс риск-менеджмента на предприятии.
- Методика проведения аудита информационной безопасности на предприятии. Три подхода к проведению аудита ИБ.
- Задачи и содержание работ при проведении аудита ИБ.
- Подготовка предприятий к проведению аудита ИБ.
- Планирование процедуры аудита ИБ на предприятии.
- Организация и проведения работ по аудиту ИБ на предприятии.
- Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ на предприятии.

Перечень вопросов к рейтинг-контролю №3

- Подготовка предприятий к проведению аудита ИБ.
- Планирование процедуры аудита ИБ на предприятии.
- Организация и проведения работ по аудиту ИБ на предприятии.
- Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ на предприятии.
- Выработка рекомендаций и подготовка отчетных документов аудита ИБ на предприятии. Экономическая оценка обеспечения ИБ предприятия.
- Программные средства для проведения аудита информационной безопасности Сравнительный анализ видов используемых программных продуктов.
- Программные средства для проведения аудита информационной безопасности. Система CRAMM.
- Программные средства для проведения аудита информационной безопасности. Система КОНДОР.
- Использование сетевых сканеров для проведения аудита информационной безопасности.

Семестр 2

Перечень вопросов к рейтинг-контролю №1

- Концепция построения системы безопасности предприятия. Защита информации в системе безопасности предприятия.
- Концептуальные модели компонентов системы безопасности предприятия.
- Принципы построения системы безопасности предприятия.
- Особенности применения средств защиты для обеспечения безопасности системы электронного документооборота (СЭД).
- Средства защиты информации для управление доступом в защищенной СЭД.
- Контроль целостности объектов СЭД.
- Криптографические средства и методы защиты информации и персональных данных в СЭД. Межсетевое экранирование и антивирусная защита для обеспечения безопасности СЭД.
- Защита данных в облачных системах работы с электронными документами СЭД.
- Безопасность мобильных устройств, применяемых в СЭД. Защита данных на сетевом и транспортном уровне.
- Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы службы безопасности предприятия.

- Виды нормативных документов службы безопасности предприятия.
- Лицензирование видов деятельности службы безопасности предприятия.

Перечень вопросов к рейтинг-контролю №2

- Рекомендации по разработке уставных документов службы безопасности предприятия.
- Организационное проектирование деятельности службы безопасности предприятия. Основы организационного проектирования систем управления.
- Методика проектирования функционального содержания управленческой деятельности.
- Методика проектирования организационной структуры системы управления.
- Методика оформления основных документов организационного проекта системы управления.
- Структура и функции службы безопасности предприятия. Состав службы безопасности предприятия. Основные функции службы безопасности предприятия.
- Построение структурной схемы управления службой безопасности предприятия.
- Основные подразделения службы безопасности предприятия.
- Функции подразделения режима и охраны.
- Функции подразделения информационно-аналитической деятельности.
- Функции режимно-секретного подразделения.
- Функции подразделения инженерно-технической защиты.

Перечень вопросов к рейтинг-контролю №3

- Организация службы защиты информации. Создание СЗИ. Структура СЗИ.
- Организационно-технические мероприятия СЗИ.
- Руководитель службы защиты информации, его права и обязанности.
- Методика разработки должностных инструкций для специалистов по защите информации.
- Управление службой безопасности предприятия (СБП). Методы управления СБП.
- Функции процессов управления СПБ. Принципы управления СБП.
- Обеспечение деятельности службы безопасности предприятия. Управление безопасностью предприятия в кризисных ситуациях.
- Подбор, расстановка и обучение сотрудников службы защиты информации.
- Роль персонала в системе защиты информации. Набор и отбор персонала в СБП.
- Требования к специалистам по защите информации. Организация обучения специалистов по защите информации.
- Требования к начальнику службы безопасности предприятия. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия.

5.2. Промежуточная аттестация

Семестр 1

Примерный перечень вопросов к экзамену

1. Парадигма системы управления информационной безопасностью.
2. Роль информационной безопасности, как процесса. Цикл Шухарта–Деминга.
3. Процессный подход в управлении информационной безопасностью.
4. Документированность системы управления информационной безопасностью.
5. Организационно-технические требования системы управления информационной безопасностью.
6. Оценивание риска в информационных системах на основе объективных оценок для повышения достоверности при расчете экспертных оценок.
7. Алгоритм расчета объективной вероятности реализаций неблагоприятных событий в компьютерной системе
8. Объективная стоимостная оценка предсказания величины ущерба от нарушений безопасности ИР. Группы контролей безопасности

9. Использование алгоритма фильтра Калмана для оценки величины ущерба от нарушений безопасности ИР. Случай взаимно-коррелированных шумов динамики и измерителя
10. Оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации.
11. Анализ защищенности информационных ресурсов предприятия.
12. Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Постановка задачи.
13. Оптимальный выбор средств комплексной системы защиты информации от возможных угроз информационной безопасности. Методика решения задачи.
14. Методология менеджмента риска. Основные понятия управления риском на предприятии. Принципы управления риском на предприятии.
15. Концепция проведения менеджмента риска на предприятии. Процесс риск-менеджмента на предприятии.
16. Методика проведения аудита информационной безопасности на предприятии. Три подхода к проведению аудита ИБ.
17. Задачи и содержание работ при проведении аудита ИБ.
18. Подготовка предприятий к проведению аудита ИБ.
19. Планирование процедуры аудита ИБ на предприятии.
20. Организация и проведения работ по аудиту ИБ на предприятии.
21. Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ на предприятии.
22. Выработка рекомендаций и подготовка отчетных документов аудита ИБ на предприятии. Экономическая оценка обеспечения ИБ предприятия.
23. Программные средства для проведения аудита информационной безопасности Сравнительный анализ видов используемых программных продуктов.
24. Программные средства для проведения аудита информационной безопасности. Система CRAMM.
25. Программные средства для проведения аудита информационной безопасности. Система КОНДОР.
26. Использование сетевых сканеров для проведения аудита информационной безопасности.

Семестр 2

Примерный перечень вопросов к экзамену

1. Концепция построения системы безопасности предприятия. Защита информации в системе безопасности предприятия.
2. Концептуальные модели компонентов системы безопасности предприятия.
3. Принципы построения системы безопасности предприятия.
4. Особенности применения средств защиты для обеспечения безопасности системы электронного документооборота (СЭД).
5. Средства защиты информации для управление доступом в защищенной СЭД.
6. Контроль целостности объектов СЭД.
7. Криптографические средства и методы защиты информации и персональных данных в СЭД. Межсетевое экранирование и антивирусная защита для обеспечения безопасности СЭД.
8. Защита данных в облачных системах работы с электронными документами СЭД.
9. Безопасность мобильных устройств, применяемых в СЭД. Защита данных на сетевом и транспортном уровне.
10. Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы службы безопасности предприятия.
11. Виды нормативных документов службы безопасности предприятия.
12. Лицензирование видов деятельности службы безопасности предприятия.
13. Рекомендации по разработке уставных документов службы безопасности предприятия.

14. Организационное проектирование деятельности службы безопасности предприятия. Основы организационного проектирования систем управления.
15. Методика проектирования функционального содержания управленческой деятельности.
16. Методика проектирования организационной структуры системы управления.
17. Методика оформления основных документов организационного проекта системы управления.
18. Структура и функции службы безопасности предприятия. Состав службы безопасности предприятия. Основные функции службы безопасности предприятия.
19. Построение структурной схемы управления службой безопасности предприятия.
20. Основные подразделения службы безопасности предприятия.
21. Функции подразделения режима и охраны.
22. Функции подразделения информационно-аналитической деятельности.
23. Функции режимно-секретного подразделения.
24. Функции подразделения инженерно-технической защиты.
25. Организация службы защиты информации. Создание СЗИ. Структура СЗИ.
26. Организационно-технические мероприятия СЗИ.
27. Руководитель службы защиты информации, его права и обязанности.
28. Методика разработки должностных инструкций для специалистов по защите информации.
29. Управление службой безопасности предприятия (СБП). Методы управления СБП.
30. Функции процессов управления СПБ. Принципы управления СБП.
31. Обеспечение деятельности службы безопасности предприятия. Управление безопасностью предприятия в кризисных ситуациях.
32. Подбор, расстановка и обучение сотрудников службы защиты информации.
33. Роль персонала в системе защиты информации. Набор и отбор персонала в СБП.
34. Требования к специалистам по защите информации. Организация обучения специалистов по защите информации.

Требования к начальнику службы безопасности предприятия. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия.

5.3. Самостоятельная работа обучающегося.

Примерная тема курсовой работы (по вариантам)

Комплексная оценка состояния информационной безопасности АИС предприятия (по вариантам). В том числе: формирование перечня защищаемой информации на предприятии (по вариантам); формирование матрицы и модели доступа к управлению информационной безопасностью; классификация АИС предприятия; определение класса защищенности информационной системы предприятия; формирование модели нарушителя информационной безопасности в АИС на предприятии; составление частной модели угроз для АИС предприятия (по вариантам) согласно методике оценки угроз безопасности информации ФСТЭК России (утверждена 05.02.2021); формирование политики ИБ в организации; проведение оценки рисков информационной безопасности предприятия.

Семестр 1

Примерные вопросы и задания для самостоятельной работы студентов

- Основные объекты инфологической модели объекта Перечень наиболее распространенных угроз. Основные компоненты модели угроз организации.
- Основные источники возникновения угроз. Возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников. Цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
- Модели оценки вероятности осуществления угрозы. Основные метрики, используемые для оценки вероятности осуществления угрозы. Способы предупреждения возможных угроз.

- Способы обнаружения угроз. Способы пресечения или локализации угроз. Действия способа ликвидации последствий.
- Защитные действия при реализации способов ЗИ. Три группы мероприятий по технической защите информации. Основные организационные мероприятия по технической защите информации.
- Роль руководителя организации в процессе управления рисками информационной безопасности. Роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности. Этапы процесса управления рисками.
- Этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками. Основные шаги анализа угроз в процедуре управления рисками.
- Этап оценки рисков в процедуре управления рисками. Этап выбора защитных мер в процедуре управления рисками. Этап реализации и проверки выбранных мер защиты в процедуре управления рисками.
- Возможности в процессе ограничения (нейтрализации) риска. Возможности в процессе переадресации риска. Оценка экономической эффективности. План реализации контрмер.
- Трактовка и способы вычисления рисков. Представление рисков в виде дерева уязвимостей, угроз и контрмер.

Семестр 2

Примерные вопросы и задания для самостоятельной работы студентов

- Служба защиты информации как составная часть системы защиты и как орган управления защитой информации. Концепция построения системы безопасности предприятия;
- Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы системы безопасности предприятия. Виды нормативных документов;
- Организационные задачи службы защиты информации. Функции службы защиты информации;
- Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации;
- Структурная схема службы защиты информации. Должностной состав сотрудников службы защиты информации. Виды и типы организационных структур службы защиты информации;
- Задачи, функции, права и ответственность сотрудников службы защиты информации;
- Порядок создания службы защиты информации;
- Структура и содержание положения о службе защиты информации;
- Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации;
- Требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров для службы защиты информации;
- Формы повышения квалификации персонала и подготовка кадрового резерва;
- Особенности деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации;
- Структура и содержание должностных инструкций сотрудников службы защиты информации;
- Принципы управления службой защиты информации. Система методов управления;
- Виды планирования и их назначение. Содержание и структура планов;
- Организация и технология планирования. Методы и формы контроля выполнения планов;
- Методы оценки эффективности и качества службы защиты информации;

- Выбор оборудования и технических средств для оснащения рабочих мест сотрудников службы безопасности и обеспечения их деятельности;
- Организация взаимодействия и сотрудничества службы безопасности предприятия с силовыми структурами региона;
- Направления развития методов и средств безопасности предприятия

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература*		
Чекулаева, Е. Н. Управление информационной безопасностью: учебное пособие: [16+] / Е. Н. Чекулаева, Е. С. Кубашева; Поволжский государственный технологический университет. – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 156 с. ISBN 978-5-8158-2165-1	2020	https://biblioclub.ru/index.php?page=book&id=612591 (дата обращения: 25.08.2021)
Шилов, А. К. Управление информационной безопасностью: учебное пособие: [16+] / А. К. Шилов; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. ISBN 978-5-9275-2742-7	2018	https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 25.08.2021)
Абденов, А. Современные системы управления информационной безопасностью: учебное пособие: [16+] / А. Абденов, Г. Дронова, В. Трушин; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2017. – 48 с. ISBN 978-5-7782-3236-5	2017	https://biblioclub.ru/index.php?page=book&id=574594 (дата обращения: 25.08.2021)
Веселов, Г. Е. Менеджмент риска информационной безопасности: учебное пособие / Г. Е. Веселов, Е. С. Абрамов, А. К. Шилов; Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Южный федеральный университет, 2016. – 109 с.ISBN 978-5-9275-2327-5	2016	https://biblioclub.ru/index.php?page=book&id=493331 (дата обращения: 25.08.2021)
Аверченков, В. И. Аудит информационной безопасности: учебное пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – Москва: ФЛИНТА, 2016. – 269 с. ISBN 978-5-9765-1256-6	2016	https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 25.08.2021)
Дополнительная литература		
Аверченков, В. И. Служба защиты информации: организация и управление: [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва: ФЛИНТА, 2016. – 186 с. ISBN 978-5-9765-1271-9	2016	https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 25.08.2021)
Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 253 с. ISBN 978-5-4475-3946-7	2015	https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 27.08.2021)

Организация безопасной работы информационных систем: учебное пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако и др.; Тамбовский государственный технический университет. – Тамбов: Тамбовский государственный технический университет (ТГТУ), 2014. – 132 с.	2013	https://biblioclub.ru/index.php?page=book&id=277794 (дата обращения: 27.08.2021)
Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. -. 312 с.	2010	http://www.studentlibrary.ru/book/ISBN9785940745747.html (дата обращения: 25.08.2021)
Санникова, И. Н. Экономическая безопасность: учебное пособие: [16+] / И. Н. Санникова, Е. А. Приходько; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2018. – 103 с. ISBN 978-5-7782-3693-6	2018	https://biblioclub.ru/index.php?page=book&id=575023 (дата обращения: 27.08.2021)

6.2. Периодические издания

1. Электронный журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html
2. Электронный журнал «Спецтехника и Связь», Режим доступа: http://www.st-s.su/
3. Электронный журнал «Системы безопасности связи и телекоммуникаций» –компания «Гротек», Москва [Электронный ресурс] // URL: http://sccs.intelgr.com/
4. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: http://www.ess.ru/
5. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: http://asbgroup.ru/izdaniya/zhurnal-bdi/

6.3. Интернет-ресурсы

1. Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: http://spymarket.com/
2. Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: http://www.mascom.ru/ (дата обращения: 13.06.2018).
3. Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: https://www.nelk.ru/
4. Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: http://www.sinf.ru/
5. Сайт компании «Проминформзащита» г. Москва [Электронный ресурс] // URL: http://www.profinfo.ru/
6. Сайт компании «Сюртель» г. Москва [Электронный ресурс] // URL: http://www.suritel.ru/
7. ЗАО ПФ «Элвира» Московская обл. г. Железнодорожный [Электронный ресурс] // URL: http://www.elvira.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред

разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил _____ доцент кафедры ИЗИ Тельный А.В.
(ФИО, должность, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр» к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 9 от 17.02.23 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»
Протокол № 9 от 17.02.23 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, должность, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Управление информационной безопасностью

образовательной программы направления подготовки 10.04.01 «Информационная безопасность»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю. Монахов/_____

Подпись *ФИО*