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

УТВЕРЖДАЮ
Руководитель программы аспирантуры

_____ А.А. Южаков
д.т.н., профессор кафедры АТ

«20» «мая» 2022 г.

Рабочая программа дисциплины по программе аспирантуры

«Управление и система управления информационной безопасностью»

Научная специальность	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность (профиль) программы аспирантуры	Информационная безопасность умного города
Выпускающая(ие) кафедра(ы)	Автоматика и телемеханика (АТ)
Форма обучения	Очная
Курс: 2	**Семестр (ы):** 3

Виды контроля с указанием семестра:
Зачет: **3** Зачет: Зачет

Пермь 2022

1. Общие положения

Рабочая программа дисциплины «Управление и система управления информационной безопасностью» разработана на основании следующих нормативных документов:

- Приказ Минобрнауки России от 20.10.2021 № 951 "Об утверждении федеральных государственных требований к структуре программ подготовки научных и научно-педагогических кадров в аспирантуре (адъюнктуре), условиям их реализации, срокам освоения этих программ с учетом различных форм обучения, образовательных технологий и особенностей отдельных категорий аспирантов (адъюнктов)";
- Постановление Правительства РФ от 30.11.2021 № 2122 "Об утверждении Положения о подготовке научных и научно-педагогических кадров в аспирантуре (адъюнктуре)";
- Самостоятельно устанавливаемые требования к реализуемым программам подготовки научных и научно-педагогических кадров в аспирантуре Пермского национального исследовательского политехнического университета;
- Базовый план по программе аспирантуры;
- Паспорт научной специальности.

1.1 Цель учебной дисциплины – формирование комплекса знаний, умений и навыков в области управления информационной безопасностью, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) объекта информатизации.

1.2 Место учебной дисциплины в структуре образовательной программы

Дисциплина «Управление и система управления информационной безопасностью» является обязательной дисциплиной образовательного компонента плана аспиранта.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения дисциплины аспирант должен демонстрировать следующие результаты:

Знать:

- принципы построения СУИБ;
- принципы разработки процессов управления ИБ;
- взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;
- подходы к интеграции СУИБ в общую систему управления объектом.

Уметь:

- практически решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять СУИБ и оценивать ее эффективность.

Владеть:

- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
- навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.

3. Структура учебной дисциплины по видам и формам учебной работы

Таблица 1

Объем и виды учебной работы

№ п.п.	Вид учебной работы	Трудоемкость, ч
		3 семестр
1	Аудиторная работа	17
	В том числе:	
	Лекции (Л)	5
	Практические занятия (ПЗ)	6
2	Контроль самостоятельной работы (КСР)	6
	Самостоятельная работа (СР)	55
	Форма итогового контроля:	Зачет

4. Содержание учебной дисциплины

4.1. Содержание разделов и тем учебной дисциплины

Раздел 1. Основы управления ИБ

(Л – 1, ПР -2 , СР –18)

Тема 1. ***Базовые вопросы управления ИБ.*** Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны.

Раздел 2. Система управления ИБ

(Л – 2, ПР -2 , СР –19)

Тема 2. ***Понятие и область деятельности СУИБ***. Понятие СУИБ. Место СУИБ в рамках общей системы управления объектом защиты. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности. Описание области деятельности.

Тема 3. ***Ролевая структура и политика СУИБ***. Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.

Раздел 3. Основы управления рисками ИБ

(Л – 2, ПР -2 , СР –18)

Тема 5. ***Управление рисками ИБ.*** Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Тема 6. ***Процессы управления ИБ.*** Процессный подход. Основные процессы СУИБ. Обязательная документация СУИБ. Процессы улучшения СУИБ. Процесс «Мониторинг эффективности». Процесс «Обучение и обеспечение осведомленности». Внедрение разработанных процессов. Внедрение мер (контрольных процедур) по обеспечению ИБ

Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса. Эксплуатация и независимый аудит СУИБ.

4.2. Перечень тем практических занятий

Таблица 2

Темы практических занятий (из пункта 4.1)

№ п.п.	Номер темы дисциплины	Наименование темы практического занятия	Наименование оценочного средства	Представление оценочного средства
1	1	Выбор области действия СУИБ Разработка Политики ИБ	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.
2	2	Разработка методики оценки рисков ИБ	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.
3	3	Проведение внутреннего аудита ИБ	Собеседование. Творческое задание.	Вопросы по темам / разделам дисциплины. Темы творческих заданий.

4.3. Перечень тем для самостоятельной работы аспирантов

Самостоятельная работа аспирантов заключается в теоретическом изучении конкретных вопросов и выполнении творческих заданий.

Таблица 3

Темы самостоятельных заданий

№ п.п.	Номер темы дисциплины	Наименование темы самостоятельной работы	Наименование оценочного средства	Представление оценочного средства
1	1	Семейства стандартов ISO/IEC 27000, СТО БР ИББС, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, BS 25999 Законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ.	Собеседование	Вопросы по темам / разделам дисциплины
2	2	Структура и содержание Политики СУИБ Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик.	Творческое задание	Темы творческих заданий
3	3	Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»).	Творческое задание	Темы творческих заданий

		Документирование процесса внедрения разработанных процессов.		

5. Методические указания для аспирантов по изучению дисциплины

При изучении дисциплины «Управление и система управления информационной безопасностью» аспирантам 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. Вся тематика вопросов, изучаемых самостоятельно, задается 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, библиотечно-справочного и информационного, информационно-справочного обеспечения для работы аспиранта по дисциплине

6.1. Библиотечные фонды и библиотечно-справочные системы

№ 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 неперерывностью 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. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

6.2.1. Информационные и информационно-справочные системы

Наименование	Ссылка на информационный ресурс
Электронно-библиотечеая 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. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

7.1. Основное учебное оборудование. Рабочее место аспиранта.

Таблица 4

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката, лабораторное оборудование)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	2	3	4	5
1	Персональные компьютеры (локальная компьютерная сеть)	12	Оперативное управление	308
2	Проектор	1	Собственность	308

8. Фонд оценочных средств

Освоение учебного материала дисциплины запланировано в течение одного семестра. Формой контроля освоения результатов обучения по дисциплине является зачет, проводимый с учетом результатов текущего контроля.

8.1. Описание показателей и критериев оценивания, описание шкал оценивания.

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию аспирантов

Текущий контроль

Текущий контроль успеваемости обеспечивает оценку освоения дисциплин и проводится в форме собеседования и защиты отчета о творческом задании.

- **Собеседование**

Для оценки **знаний** аспирантов проводится собеседование в виде специальной беседы преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной для выяснения объема знаний по определенному разделу, теме, проблеме.

Собеседование может выполняться в индивидуальном порядке или группой аспирантов.

- **Защита отчета о творческом задании**

Для оценки **умений и владений** аспирантов используется творческое задание, имеющее нестандартное решение и позволяющее интегрировать знания различных областей, аргументировать собственную точку зрения.

Творческие задания могут выполняться в индивидуальном порядке или группой аспирантов.

Промежуточная аттестация

Допуск к промежуточной аттестации осуществляется по результатам текущего контроля. Промежуточная аттестация проводится в виде зачета по дисциплине, в устно-письменной форме по билетам. Билет содержит теоретические вопросы (ТВ) и практическое задание (ПЗ).

Билет формируется таким образом, чтобы в него попали вопросы и практические задания. Пример билета представлен в приложении 1.

Шкалы оценивания результатов обучения при сдаче зачета:

Оценка результатов обучения по дисциплине проводится по 5-балльной системе оценивания путем выборочного контроля во время зачета.

Шкалы и критерии оценки результатов обучения при сдаче зачета приведены в табл. 5.

Таблица 5

Шкала оценивания результатов освоения на зачете

Оценка	Критерии оценивания
Зачтено	Аспирант продемонстрировал сформированные и систематические знания при ответе на теоретический вопрос билета. Показал отличные **знания** в рамках усвоенного учебного материала. Ответил на все или большинство дополнительных вопросов. Аспирант правильно выполнил контрольное задание билета. Показал успешное и систематическое **применение** полученных знаний и **умений** при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все или большинство дополнительных вопросов.
Не зачтено	При ответе на теоретический вопрос билета аспирант продемонстрировал фрагментарные **знания** при ответе на теоретический вопрос билета. При ответах на дополнительные вопросы было допущено множество неправильных ответов. При выполнении контрольного задания билета аспирант продемонстрировал частично

Оценка	Критерии оценивания
	освоенное **умение** и **применение** полученных навыков при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено множество неточностей.

9. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

Задания для текущего контроля и проведения промежуточной аттестации должны быть направлены на оценивание:

1. Уровня освоения теоретических понятий, научных основ профессиональной деятельности;
2. Степени готовности аспиранта применять теоретические знания и профессионально значимую информацию и оценивание сформированности когнитивных умений.
3. Приобретенных умений, профессионально значимых для профессиональной деятельности.

10. Типовые контрольные вопросы и задания или иные материалы, необходимые для оценки результатов освоения дисциплины

Перечень контрольных вопросов и заданий для сдачи зачета по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность разработан с учетом научных достижений научно-исследовательской школы кафедры.

Типовые творческие задания:

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. Содержание и жизненный цикл политики ИБ.
5. Уровни процесса управления ИБ.
6. Процессный подход для управления ИБ и его составляющие.
7. Система управления информационной безопасностью (СУИБ) организации и цель ее разработки. Требования к СУИБ.
8. Процессный подход управления ИБ. Цикл PDCA и его компоненты.
9. Характеристика этапов создания СУИБ и их логическая взаимосвязь.
10. Содержание документации для создания СУИБ предприятия (организации).
11. Управление рисками ИБ. Подходы к управлению рисками ИБ.
12. Содержание процесса управления рисками ИБ. Соответствие цикла СУИБ и PDCA.
13. Управление инцидентами ИБ. Цели организации по управлению инцидентами ИБ.
14. Этапы процесса управления инцидентами ИБ, в соответствии с моделью PDCA.
15. Программа аудита ИБ. Управление программой аудита ИБ.
16. Измерение эффективности СУ ИБ. Метрики эффективности.

Типовые контрольные задания:

1. Осуществить разработку Политики информационной безопасности.
2. Разработать систему управления информационной безопасностью, с учетом выбранной в рамках области действия СУИБ.
3. Разработать Методику анализа и оценки рисков информационной безопасности для систем управления информационной безопасностью.
4. Провести обработку рисков информационной безопасности в соответствии с выбранной областью действия СУИБ и активами.
5. Сформировать основные положения Политики управления инцидентами информационной безопасности для предприятия (организации).
6. Разработать макет Программы аудита предприятия (организации).

Полный комплект вопросов и заданий хранится на кафедре «АТ».

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1		
2		
3		
4		