Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Северо-Западный институт управления – филиал РАНХиГС

Кафедра бизнес-информатики

УТВЕРЖДЕНО
Директор СЗИУ РАНХиГС
А.Д.Хлутков

ПРОГРАММА МАГИСТРАТУРЫ
Аналитическое обеспечение информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04 Организационное и правовое обеспечение информационной безопасности

(индекс, наименование дисциплины, в соответствии с учебным планом)

38.04.05 Бизнес-информатика
(код, наименование направления подготовки (специальности)

Очная
(форма обучения)

Год набора – 2024

Санкт-Петербург, 2024 г.

Автор-составитель:
Кандидат технических наук, кандидат педагогических наук, доцент,
доцент кафедры бизнес-информатики Сухостат Валентина Васильевна

Заведующий кафедрой «Бизнес-информатика»
Доктор военных наук, кандидат технических наук,
профессор, Наумов Владимир Николаевич

В новой редакции РПД Б1.В.04 «Организационное и правовое обеспечение информационной безопасности» одобрена протоколом № 10 заседания кафедры бизнес-информатики от 26.06.2024 г
.

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.04 «Организационное и правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями:

Таблица 1.1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКс-4	Способен управлять информационными сервисами, ресурсами ИТ и ИТ-инновациями. Управлять ИАС в защищенном исполнении, обслуживать системы защиты	ПКс-4.2	Способен управлять ИАС в защищенном исполнении

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 1.2

ОТФ/ТФ *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения
Выполнение трудовой функции «Управление информационной безопасностью ресурсов ИТ» в соответствии с обобщенной трудовой функцией профессионального стандарта 06.014 «Менеджер информационных технологий» - управление ресурсами ИТ. Управление бизнес-анализом 06.031 «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности»	ПКс-4.2	на уровне знаний*:* **Знать:** – основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – правовые основы организации защиты государственной тайны и конфиденциальной информации задачи органов защиты государственного регулирования; – правовые нормы и стандарты по лицензированию в области обеспечения защиты конфиденциальной информации и сертификации средств защиты информации; – принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности на предприятии; – правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); – понятие, сущность и принципы управления информационного сервиса, информационных ресурсов, подлежащих защите на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
		на уровне умений: **Уметь:** – осуществлять организационное и правовое обеспечение информационной безопасности информационного

		сервиса, ресурсов ИТ в рамках должностных обязанностей менеджера ИТ/специалиста по автоматизации информационно-аналитической деятельности в сфере безопасности; – применять нормативные правовые акты и нормативные методические документы в области защиты информации; – выявлять каналы утечки информации на объекте защиты и контролировать соблюдение персоналом требований режима защиты информации; – оформлять документацию по регламентации мероприятий и оказанию услуг в области информационной безопасности защиты информации; – определять виды и формы информации, подверженной угрозам, возможные угрозы и риски информационной безопасности; выявлять требования и ограничения информационной безопасности с учетом соответствия концептуальной модели системы; – применять средства обеспечения информационной безопасности в системах управления базами данных, компьютерных сетях на основе анализа данных, поддержки принятия решений.
		на уровне навыков **:** **Владеть:** – навыками организационного и правового обеспечения информационной безопасности информационного сервиса, ресурсов ИТ в рамках должностных обязанностей менеджера ИТ / специалиста по автоматизации информационно-аналитической деятельности в сфере безопасности; – навыками управления ресурсами ИТ, управления бизнес-анализом, в процессе информационно-аналитической деятельности в сфере безопасности при решении своих профессиональных задач

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы /144 академ. часа

Таблица 2

Вид работы	Трудоемкость (акад/астр.часы)
Общая трудоемкость	**144/108**
Контактная работа с преподавателем	***50/37,5***
Лекции	20/15
Практические занятия	28/21
Самостоятельная работа	**58/43,5**
Консультации	**2/1,5**
Контроль	***36/27***
Формы текущего контроля	Т,О, Зад.
Форма промежуточной аттестации	***Экзамен***

Место дисциплины в структуре ОП ВО

Дисциплина изучается в 4-м семестре 2-го курса. Дисциплина Б1.В.04 «Организационное и правовое обеспечение информационной безопасности» относится к части дисциплин, формируемых участниками образовательных отношений учебного плана по направлению 38.04.05 Бизнес-информатика образовательной программы «Аналитическое обеспечение информационной безопасности». Преподавание дисциплины опирается на дисциплины программы магистратуры Б1.В.01 «Управление информационной безопасностью», Б1.В.05 «Методы бизнес-аналитики».

Дисциплина закладывает теоретический и методологический фундамент для овладения умениям и навыками в ходе овладения дисциплинами (модулями) по выбору 3 (ДВ.3), Б2.О.01(У) «Проектно-аналитическая практика» и Б2.О.02 (Н) «Научно-исследовательская работа».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении выпускных квалификационных работ.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Таблица 3

№ п/п	**Наименование тем**	**Объем дисциплины, час.**					**Форма текущего контроля успеваемости**, промежуточной аттестации*****
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**			**СР**	
			Л/ДОТ	**ПЗ/ДОТ**	**КСР**	СРО	
Тема 1	Теоретические основы организационного и правового обеспечения информационной безопасности	34	6	8		20	Т(О)*
Тема 2	Правовое обеспечение информационной безопасности	38	8	10		20	О(Т)**
Тема 3	Организационное обеспечение информационной безопасности	34	6	10		18	Т(О)*, Зад
Промежуточная аттестация		36/27			2*		Экзамен
Всего (акад./астр. часы):		106/82	20/15	28/21	2/1,5	58/45	

Используемые сокращения:
Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся)[1];
ЛР – лабораторные работы (вид занятий семинарского типа)[2];
ПЗ – практические занятия (виды занятий семинарского типа за исключением лабораторных работ)[3];
КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации)[4];
ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.
СРО – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.
Примечание:
** – разработчик указывает формы заданий текущего контроля успеваемости (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.), с применением которых ведется мониторинг успешности освоения образовательной программы обучающимися*
*** – разработчик указывает формы промежуточной аттестации: экзамен (Экз), зачет (З)/ зачет с оценкой (ЗО).*
Используемые сокращения и примечания включаются после каждой из заполняемых таблиц.

3.2. Содержание дисциплины

Тема 1. Теоретические основы организационного и правового обеспечения информационной безопасности

Основы обеспечения информационной безопасности. Основные сферы общественной жизни: экономическая сфера, социальная сфера, сфера духовной жизни, сфера государственного управления.

Понятие «информационная сфера». Информационная сфера. Субъектный сегмент. Общественный сегмент. Смешанный сегмент информационной инфраструктуры.

Обеспечение информационной безопасности. Обеспечение безопасности: базовые

---

[1] Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

[2] См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

[3] См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

[4] Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

понятия. Обеспечение ИБ организации. Правовое обеспечение ИБ. Организационное обеспечение ИБ. Средства технического, кадрового, материального, финансового, информационного и научного обеспечения ИБ ВФ.

Тема 2. Правовое обеспечение информационной безопасности.

Понятие и содержание правового обеспечения ИБ. Место информационной безопасности в национальной безопасности РФ.

Информация как объект правоотношений в сфере обеспечения ИБ. Информационные технологии и защита информации.

Государственная тайна как особый вид защищаемой информации.

Правовое регулирование защиты сведений конфиденциального характера. Безопасность персональных данных. Служебная тайна как вид защищаемой информации. Коммерческая тайна и правовой режим обеспечения ее безопасности. Правовое регулирование защиты сведений профессиональной деятельности.

Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности. Общие положения. Интеллектуальные права и правовое обеспечение безопасности их использования. Основы авторского и смежного права. Основы патентного права. Право промышленной собственности. Электронная подпись и правовое обеспечение безопасности переписки.

Правовое обеспечение защиты критической информационной инфраструктуры.

Обеспечение безопасности при использовании сетей связи и сети Интернет. Техническое регулирование и требования по безопасности информационных технологий.

Юридическая ответственность за правонарушения в области информации, информационных технологий и защиты информации. Понятие и виды юридической ответственности. Судебная защита прав и свобод человека и гражданина в информационной сфере. Уголовно-правовая ответственность в сфере компьютерной информации.

Тема 3. Организационное обеспечение информационной безопасности.

Понятие, сущность и содержание организационного обеспечения ИБ. Организационная основа государственной системы обеспечения ИБ, полномочия органов государственной власти. Цель, принципы и приоритеты государственной политики в области технической защиты информации.

Государственная система лицензирования. Лицензирование в области обеспечения ИБ. Общие подходы и принципы организации безопасности предприятия и системы управления рисками.

Организация и порядок сертификации продукции в системе Федеральной службы по техническому контролю. Организация и порядок сертификации продукции в системе Федеральной службы безопасности.

Аттестация объектов информатизации по требованиям безопасности информации. Порядок проведения аттестации объектов информатизации. Требования к нормативным и методическим документам по аттестации объектов информатизации.

4. Материалы текущего контроля успеваемости обучающихся

В ходе реализации дисциплины Б1.В.04. «Организационное и правовое обеспечение информационной безопасности» используются следующие **методы текущего контроля успеваемости** обучающихся:

Таблица 3.1

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Теоретические основы организационного и правового обеспечения информационной безопасности	Тестирование, опрос
Тема 2. Правовое обеспечение информационной безопасности	Тестирование, опрос
Тема 3. Организационное обеспечение информационной безопасности	Тестирование, опрос, задание

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Типовые оценочные материалы по теме 1

Типовые вопросы для опроса по теме 1

1. Назовите основные сферы общественной жизнедеятельности. Охарактеризуйте механизмы влияния ИКТ на их развитие.
2. Дайте определение понятия «информационная сфера» и охарактеризуйте ее структуру.
3. Раскройте понятия «информационная безопасность» и «обеспечение информационной безопасности».
4. Что такое правовое обеспечение ИБ?
5. Что такое организационное обеспечение ИБ?
6. Дать определение понятия «право». Роль права в регулировании общественных отношений.
7. Назовите основные виды норм права, объясните их структуру.
8. Охарактеризуйте формы и содержание правового обеспечения ИБ.
9. Дайте определение понятия «источники права». Каковы источники права в области обеспечения ИБ?
10. Назовите существующие виды информации.
11. Что составляет организационную основу системы обеспечения информационной безопасности РФ.
12. Раскройте основные функции системы обеспечения информационной безопасности РФ.
13. Охарактеризовать структуру, принципы организации и особенности работы по защите государственной тайны.

Тест:

1. К основным сегментам информационной инфраструктуры НЕ относится:
    1) автономный;
    2) субъектный;
    3) общественный;
    4) смешанный.
2. Юридические лица, являющиеся коммерческими организациями, могут создаваться
    1) в форме хозяйственных товариществ и обществ, производственных кооперативов, государственных и муниципальных унитарных предприятий;

2) в форме потребительских кооперативов, общественных или религиозных организаций (объединений), финансируемых собственником учреждений, благотворительных или иных фондов.

3. Угроза информационной безопасности – это … воздействие на информационную систему
   1) потенциально возможное;
   2) уже произошедшее;
   3) реализуемое в настоящее время .
4. «Информационное измерение» государства определяется
   1) ролью и местом информации и информационной инфраструктуры в деятельности государственных органов и организаций по выполнению функций государства;
   2) деятельностью его органов по стимулированию развития информационной инфраструктуры и активной информационной деятельности граждан по защите их прав и свобод в этой области.
5. Основными составляющими правового обеспечения информационной безопасности являются:
   1) планирование использования и управления применением материальных, людских, финансовых и др. ресурсов, выделяемых для противодействия угрозам, связанных с информацией и информационной инфраструктурой;
   2) совокупность норм права;
   3) правоприменительная практика.

Типовые оценочные материалы по теме 2

Типовые вопросы для опроса по теме 2:

1. Раскрыть содержание предметной сферы законодательства в области информации, информационных технологий и защиты информации.
2. Каким образом осуществляется распространение (предоставление) информации в Российской Федерации?
3. Что предусматривает государственное регулирование в сфере применения информационных технологий?
4. Раскрыть основные объекты регулированных правом общественных отношений в сети Интернет.
5. Дать определение понятию «персональные данные». Какие сведения относятся к персональным данным?
6. Что составляет предмет и в чем заключается цель правового регулирования в области персональных данных?
7. Раскрыть принципы и условия обработки персональных данных, их конфиденциальность.
8. Раскрыть организацию контроля и надзора соблюдения законодательства в области персональных данных.
9. Перечислить основные источники права в области интеллектуальной собственности.
10. Раскрыть основное содержание источников права в области интеллектуальной собственности.
11. Назвать основные способы правовой защиты интеллектуальных прав.
12. Дать определения авторского, смежного права.
13. Раскрыть содержание понятия «промышленная собственность».
14. Изложить основные способы защиты патентных прав.
15. Дать определение электронной подписи.
16. Что такое удостоверяющий центр и каковы его функции?
17. Раскрыть содержание прав и обязанностей обладателя информации, содержащей

коммерческую тайну.

18. В чем заключается предмет и цель правового регулирования отношений в области государственной тайны?
19. Как организовано государственное регулирование и надзор в области связи?
20. Что понимается под техническим регулированием и каковы цели его принятия?
21. В чем заключается разнообразие и сложность юридическго определения «компьютерные преступления»?

Тест

1. Ноу−хау, разработанные и сохраняемые фирмой в секрете, являются ее … тайной
    1) служебной;
    2) коммерческой;
    3) профессиональной.
2. … – государственный орган, на который возложены функции по лицензированию и сертификации в сфере криптографической защиты и защиты государственной тайны
    1) ФСБ;
    2) ФСТЭК;
    3) МВД.
3. Увольнение за разглашение охраняемой законом тайны предусмотрено:
    1) п.6 пп. в ст.81 ТК РФ;
    2) п.6 ст.81 ТК РФ;
    3) п.5 ст.81 ТК РФ.
4. За разглашение информации работником, работодатель вправе применить дисциплинарные взыскания:
    1) замечание;
    2) увольнение;
    3) штраф;
    4) выговор;
    5) предупреждение.
5. Выберите объекты, охраняемые нормами авторского права:
    1) программы ЭВМ;
    2) организация эфирного и кабельного телевидения;
    3) законы;
    4) произведения науки, литературы и искусства.

Типовые оценочные материалы по теме 3
Типовые вопросы для опроса по теме 3:

1. Раскрыть основу системы обеспечения информационной безопасности РФ.
2. Изложить цель, принципы и приоритеты направления государственной политики в области информационной безопасности.
3. Какие нормативные документы устанавливают порядок лицензирование деятельности в сфере защиты информации?
4. Каков общий порядок и состав представленных в лицензирующий орган документов для получения лицензии?
5. Каковы цели защиты информации?
6. Что является главным направлением работ по защите информации?
7. Что представляет собой угроза информационной безопасности?
8. Что такое риск информационной безопасности?
9. Что представляет собой процесс управления риском информационной безопасности?

10. Каковы организация и порядок сертификации продукции в системе ФСТЭК, ФСБ?
11. Изложить организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации.
12. Раскрыть требования к нормативным и методическим документам по аттестации объектов информатизации.

Тест

1. Документ, содержащий набор правил и требований, специфичных для системы или процесса, которым последние должны точно соответствовать - это
    1) стандарт безопасности;
    2) руководство безопасности;
    3) политика безопасности.
2. ISO/IEC … – международный стандарт, определяющий общие критерии оценки безопасности информационных технологий
    1) 15408;
    2) 900x;
    3) 2000x.
3. Аналитик оценки:
    1) измеряет и оценивает свидетельства оценки, предоставленными владельцами активов;
    2) выбирает способ, модель оценки и определяет методику оценки ИБ;
    3) проводит анализ результатов оценки и формирует отчет и рекомендации по результатам оценки.
4. К обеспечению безопасности информационных технологий организации должны привлекаться:
    1) все сотрудники, участвующие в процессах автоматизированной обработки информации;
    2) все категории обслуживающего АС персонала;
    3) все категории посторонних лиц.
5. Укажите, из скольких уровней состоит общая структура нормативно-методических документов компании в области информационной безопасности:
    1) из 1;
    2) из 3;
    3) из 5.

Задание: «Нормативно-правовое обеспечение ИБ. Построение концептуальной модели ИБ».

1. Составить логическую схему знаний по содержанию блока.
2. Составить терминологический словарь согласно нормативно-правовым документам и стандартам (https://fstec.ru/).
3. Провести анализ содержания основных законодательных и нормативно-правовых документов, регулирующих вопросы обеспечения ИБ на федеральном, региональном и ведомственного уровнях, используя справочно-правовую систему «Консультант Плюс».
4. Раскрыть содержание определения средств (методов) защиты информации в ФЗ.
5. Дать характеристику содержания понятия «информационная безопасность РФ» согласно Стратегии национальной безопасности.
6. Дать характеристику российских стандартов в области обеспечения информационной безопасности и перечислить их основные функции (составить таблицу).
7. Описать перечень средств защиты информации, указанных в Законе РФ «О государственной тайне».

8. Определить перечень средств защиты информации, закрепленных ФЗ-149 «Об информации, информационных технологиях и защите информации».
9. Построить концептуальную модель ИБ.
10. Предоставить отчет в виде документа и презентации.

Задание. «Разработка политики безопасности кафедры бизнес-информатики».

1. Изучить шаблоны документов, описывающих политику информационной безопасности организации, представленные в разделе " Политика безопасности " сайта SecurityPolicy.ru (основная цель проекта SecurityPolicy.ru - создание сообществом специалистов комплектов типовых документов по информационной безопасности для различных организаций, которыми могут воспользоваться все желающие без ограничений, а также подборка шаблонов документов по информационной безопасности, законодательных и нормативных актов)
2. Изучить устав и стратегические цели СЗИУ(факультета ЭиФ/ кафедры БИ).
3. Подобрать наиболее подходящий шаблон документа для описания политики безопасности ВУЗа (подразделения), при необходимости модифицировав его структуру
4. Разработать политику безопасности ВУЗа (подразделения) с учетом специфики его деятельности и планов развития.
5. Предоставить отчет в виде документа и презентации.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1 Экзамен проводится устно по билетам.

5.2 Оценочные материалы промежуточной аттестации

Таблица 5.2.1

Компонент компетенции	Промежуточный/ключевой индикатор оценивания	Критерий оценивания
Управляет ИАС в защищенном исполнении	Использует и управляет ИАС в защищенном исполнении для решения задач в области информационной безопасности.	Самостоятельно определяет потребности и рекомендации решений, которые обеспечивают ценность для заинтересованных лиц в рамках задач взаимодействия областей информационной безопасности и бизнеса

Типовые оценочные материалы промежуточной аттестации

Вопросы к экзамену

по дисциплине Б1.В.04 «Организационное и правовое обеспечение информационной безопасности»

1) Понятие «информационная сфера». Субъектный сегмент. Общественный сегмент.
2) Смешанный сегмент информационной инфраструктуры.
3) Информация как объект правоотношений в сфере обеспечения ИБ.
4) Информационные технологии и защита информации.
5) Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности. Общие положения
6) Государственное регулирование в сфере информационной безопасности.
7) Обеспечение безопасности: базовые понятия.
8) Защищенная электронная подпись. Цифровые сертификаты.
9) Интеллектуальные права и правовое обеспечение безопасности их использования
10) Основы авторского и смежного права.
11) Право промышленной собственности.

12) Обеспечение безопасности при использовании сетей связи и сети Интернет.

13) Правовое обеспечение защиты критической информационной инфраструктуры.

14) Техническое регулирование и требования по безопасности информационных технологий

15) Понятие и виды юридической ответственности.

16) Компьютерные преступления. Уголовно-правовая ответственность в сфере компьютерной информации.

17) Судебная защита прав и свобод человека и гражданина в информационной сфере.

18) Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

19) Обеспечение информационной безопасности на государственном уровне.

20) Обеспечение информационной безопасности на уровне предприятия.

21) Коммерческая тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

22) Государственная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

23) Персональные данные: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

24) Банковская тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

25) Тайна страхования: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

26) Налоговая тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

27) Врачебная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

28) Тайна переписки: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

29) Служебная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

30) Профессиональная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

31) Правовые основания отнесения сведений к категории ограниченного доступа.

32) Понятие, сущность и содержание организационного обеспечения ИБ.

33) Организационная основа государственной системы обеспечения ИБ, полномочия органов государственной власти.

34) Цель, принципы и приоритеты государственной политики в области технической защиты информации.

35) Государственная система лицензирования в области обеспечения ИБ..

36) Общие подходы и принципы организации безопасности предприятия и системы управления рисками.

37) Национальные стандарты в области информационной безопасности и защиты информации.

38) Международные стандарты в области информационной безопасности и защиты информации.

39) Организация и порядок сертификации продукции в системе Федеральной службы по техническому контролю.

40) Организация и порядок сертификации продукции в системе Федеральной службы безопасности.

41) Аттестация объектов информатизации по требованиям безопасности информации

Шкала оценивания.

Оценка результатов производится на основе Положения о текущем контроле успеваемости обучающихся и промежуточной аттестации обегающихся по образовательным программам среднего профессионального и высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академии народною хозяйства и государственной службы при Президенте Российской Федерации», утвержденного Приказом Ректора РАНХиГС при Президенте РФ от 30.01.2018 г. № 02-66 (п.10 раздела 3 (первый абзац) и п.11), а также Решения Ученого совета Северо-западного института управления РАНХиГС при Президенте РФ от 19.06.2018, протокол № 11.

Экзамен:

Оценка «отлично» выставляется в случае, если при устном ответе студент проявил (показал):

- глубокое и системное знание всего программного материала учебного курса, изложил ответ последовательно и убедительно;
- отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей дисциплины;
- умение правильно применять теоретические положения при решении практических вопросов и задач.

Оценки «хорошо» выставляется в случае, если при устном ответе студент проявил (показал):

- знание узловых проблем программы и основного содержания лекционного курса;
- умение пользоваться концептуально-понятийным аппаратом умение преимущественно правильно применять теоретические положения при решении практических вопросов и задач;
- умение выполнять предусмотренные программой задания;
- в целом логически корректное, но не всегда точное и аргументированное изложение ответа.

Оценка «удовлетворительно» выставляется в случае, если при устном ответе студент проявил (показал):

- фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины;
- затруднения с применением теоретических положений при решении практических вопросов и задач.

Оценка «неудовлетворительно» выставляется в случае, если при устном ответе студент проявил (показал):

- незнание либо отрывочное представление учебно-программного материала;
- неумение использовать научно-понятийный аппарат и терминологию учебной дисциплины;
- неумение применять теоретические положения при решении практических вопросов и задач,
- неумение выполнять предусмотренные программой задания.

6. Методические материалы по освоению дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия. На лекциях рассматриваются наиболее сложный материал дисциплины. Для развития у магистрантов креативного мышления и логики в каждой теме учебной дисциплины предусмотрены теоретические положения, инструментальные средства, а также примеры их использования при решении задач обеспечения информационной безопасности. Кроме того, часть теоретического материала предоставляется на самостоятельное изучение по рекомендованным источникам для формирования навыка самообучения.

Практические занятия предназначены для самостоятельной работы магистрантов по решению конкретных задач. Каждое практическое занятие сопровождается заданиями, выдаваемыми магистрантам для решения во внеаудиторное время.

Для работы с печатными и электронными ресурсами СЗИУ имеется возможность доступа к электронным ресурсам. Организация работы магистрантов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

Обучение по дисциплине «Организационное и правовое обеспечение информационной безопасности» предполагает изучение курса на аудиторных занятиях (лекции, практические работы) и самостоятельной работы обучающихся. Семинарские занятия дисциплины «Организационное и правовое обеспечение информационной безопасности» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

Подготовка к лекции заключается в следующих рекомендациях:

- внимательно прочитайте материал предыдущей лекции;
- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
- ознакомьтесь с учебным материалом по рекомендуемой литературе;
- постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
- запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим занятиям:

- внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом;
- ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
- уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;
- готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;
- рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

Выполнение задания:

- повторение лекционного материала, изучение нормативной литературы (текста стандарта), использование рекомендуемой литературы.
- посещение консультаций преподавателя.

Процедура осуществления контроля выполнения задания проводится по критериям.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература

1. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации: учебник / сост. И.Г. Дровникова, А. В. Калач, И.И. Лившиц, Е.А. Рогозин, А.В. Скрипников.; ФКОУ ВО Воронежский институт ФСИН России – Воронеж, ИПЦ «Научная книга», 2022. – 304 с. – Текст: электронный // ЭБС Znanium [сайт]. — URL:https://znanium.com/catalog/document?id=426504.

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/477968.

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/469235.

4. Основы управления информационной безопасностью : учебное пособие : Допущено УМО ... / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва: Горячая линия-Телеком, 2016.- 244 с. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр.: с. 234-239. - ISBN 978-5-9912-0361-6.

5. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/476798.

Все источники основной литературы взаимозаменяемы.

7.2 Дополнительная литература

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков: учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 03.08.2021). – Режим доступа: по подписке.

2. Дронов В.Ю. Международные и отечественные стандарты по информационной безопасности: учебно-методическое пособие / Дронов В.Ю.. — Новосибирск : Новосибирский государственный технический университет, 2016. — 34 с. — ISBN 978-5-7782-3112-2. — Текст : электронный // Электронно-библиотечная система

IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91395.html (дата обращения: 03.08.2021). — Режим доступа: для авторизир. Пользователей

3. Гасанов Э.С. Самарина Е.А. Управление информационной безопасностью в корпоративной предпринимательской среде в условиях киберугроз цифровой экономики [Электронный ресурс] – URL: https://cyberleninka.ru/article/n/

7.3. Нормативные правовые документы.

Не используются

7.4. Интернет-ресурсы.

СЗИУ располагает доступом через сайт научной библиотеки http://nwapa.spb.ru/ к следующим подписным электронным ресурсам:

https://ranalytics.github.io/tsa-with-r/ch-intro-to-prophet.html

Русскоязычные ресурсы

Электронные учебники электронно - библиотечной системы (ЭБС) «Айбукс»

Электронные учебники электронно – библиотечной системы (ЭБС) «Лань»

Электронные учебники электронно – библиотечной системы (ЭБС) «Юрайт»

Электронные учебники электронно – библиотечной системы (ЭБС) «Знаниум»

Рекомендуется использовать следующий интернет-ресурсы

http://serg.fedosin.ru/ts.htm

http://window.edu.ru/resource/188/64188/files/chernyshov.pdf

7.5 Иные источники.

Не используются

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Учебная дисциплина включает использование программного обеспечения пакет программ MS Office 2013, 2016, справочная электронная система «Гарант» для подготовки текстового и табличного материала.

Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы) Office 365, Teams, Moodle

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование
1.	Компьютерные классы с персональными ЭВМ, объединенными в локальные сети с выходом в Интернет
1.	Пакет Excel -2016, proffesional plus, IBM SPSS statistics, R, RStudio, Anaconda
2.	Мультимедийные средства в каждом компьютерном классе и в лекционной аудитории
3.	Браузер, сетевые коммуникационные средства для выхода в Интернет. Сервисы и службы Azure

Компьютерные классы из расчета 1 ПЭВМ для одного обучаемого. Каждому обучающемуся должна быть предоставлена возможность доступа к сетям типа Интернет в течение не менее 20% времени, отведенного на самостоятельную подготовку.