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
(наименование кафедры)

УТВЕРЖДЕНО
Директор СЗИУ РАНХиГС
А.Д. Хлутков

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.05 Информационная безопасность
(индекс, наименование дисциплины, в соответствии с учебным планом)
Часть, формируемая участниками образовательных отношений

38.03.05 Бизнес-информатика
(код,наименование направления подготовки)

«Бизнес-аналитика»
(профиль)

бакалавр
(квалификация)

очная
(форма обучения)

Год набора – 2024

Санкт-Петербург, 2024г.

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

Заведующий кафедрой бизнес информатики
Доктор военных наук, кандидат технических наук,
профессор Наумов Владимир Николаевич

РПД Б1.В.05 «Информационная безопасность» одобрена протоколом заседания кафедры бизнес-информатики № 10 от 27.06.2024 г.

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.05 «Информационная безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Таблица 1.1

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПКС-1	Способен управлять ресурсами ИТ, инфраструктурой, информационной безопасностью, качеством ИТ	ПКС-1.2	Демонстрирует умение управлять информационной безопасностью ресурсов ИТ, использовать стандарты информационной безопасности, методики и средства обеспечения информационной безопасности

В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 1.2

ОТФ/ТФ (профессиональный стандарт 06.014 Менеджер по информационным технологиям) профессиональные действия	Код компонента компетенции	Результаты обучения
3.1.6. Трудовая функция: управление информационной безопасностью. **Трудовые действия:** - формирование и согласование целей и принципов управления информационной безопасностью; - определение состава методов и средств обеспечения безопасности ИТ, соответствующих критериям оценки безопасности ИТ; - организация управления информационной безопасностью с помощью персонала и стейкхолдеров; - контроль качества и управление улучшением управления информационной безопасностью.	ПКС-1.2	**на уровне знаний**: - международные и отечественные стандарты, лучшие практики и фреймворки по управлению информационной безопасностью ресурсов ИТ; - методы и средства обеспечения безопасности ИТ, критерии оценки безопасности ИТ; - методы контроля безопасности ИТ; - методы непрерывного улучшения управления информационной безопасностью; **на уровне умений:** - формировать и декомпозировать цели управления информационной безопасностью ресурсов ИТ; - использовать методы и средства обеспечения безопасности ИТ, соответствующие критериям оценки безопасности ИТ; - формировать команду и организовывать персонал и стейкхолдеров для управления информационной безопасностью; - осуществлять мониторинг и контроль управления информационной безопасностью; - организовывать деятельность по непрерывному улучшению УИБ ресурсов ИТ; **на уровне навыков:** - решения профессиональных задач посредством частных инструментов по управлению ИБ

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	**144/110**
Контактная работа с преподавателем	***64/49,2***
Лекции	20/15,3
Практические занятия	28/21,5
Самостоятельная работа	**44/33,8**
Контроль	***36/27,6***
Формы текущего контроля	КР
Форма промежуточной аттестации	***Экзамен***

Место дисциплины в структуре ОП ВО

Дисциплина изучается в 6-м семестре 3-го курса. Дисциплина Б1.В.05 «Информационная безопасность» относится к части, формируемой участниками образовательных отношений учебного плана по направлению «Бизнес-информатика» 38.03.05. Преподавание дисциплины «Информационная безопасность» основано на дисциплинах – Б1.О.07.05 «Теория вероятностей и математическая статистика»; Б1.О.08 «Теория систем и системный анализ»; Б1.В.06 «Анализ данных». В свою очередь она создаёт необходимые предпосылки для освоения программ таких дисциплин, как Б1.О.21 «Анализ и моделирование бизнес-процессов», Б1.О.28 «Архитектура предприятия», Б1.О.21 «Управление жизненным циклом ИС» и ряда дисциплин по выбору студента

Дисциплина закладывает теоретический и методологический фундамент для овладения умениям и навыками в ходе Б2.В.01(П) Научно-исследовательская работа и Б2.В.03 (Пд) Преддипломная практика.

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

3. Содержание и 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	ПЗ	КСР	СРО	СП	
Тема 1	Нормативная база и стандарты в области ИБ и защиты информации. Компьютерная преступность	24	4	8		10	2	Т*
Тема 2	Угрозы безопасности информации	32	8	8		16		Задание (З)/Т
Тема 3	Методы и средства защиты информации от несанкционированного доступа	36	8	12		12	2	Круглый стол
Консультации		16						
Текущий контроль							4	КР
Промежуточная аттестация		*36*			2*			Экзамен
Всего (акад./астр. часы):		144/110,7	20/15,3	28/21,5	2/1,5	38/29,2	8/6	

Примечание:

2* - консультация, не входящая в общий объем дисциплины

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) ;

ПЗ – практические занятия (виды занятия семинарского типа за исключением лабораторных работ) ;

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) ;

СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях;

СП – самопроверка;

СРО – самостоятельная работа обучающегося

контрольные работы (К), опрос (О), тестирование (Т)

Содержание дисциплины

Тема 1. Нормативная база и стандарты в области информационной безопасности и защиты информации

Нормативная база информационной безопасности и защиты информации. Государственная политика в сфере информационной безопасности и защиты информации. Правовое обеспечение информационной безопасности. Конституция РФ об «информационных правах и обязанностях». Основные нормативные документы, регулирующие отношения в сфере информационной безопасности. Виды «тайн» по Российскому законодательству. Классификация тайн.

Обобщенная модель информационной безопасности. Национальные стандарты в области информационной безопасности и защиты информации. Международные стандарты в области информационной безопасности и защиты информации. Проблемы гармонизации стандартов информационной безопасности.

Понятие компьютерной преступности. Масштабы и общественная опасность компьютерной преступности. Виды и субъекты компьютерных преступлений. Специфика расследования компьютерных преступлений. Предупреждение компьютерных преступлений. Кодификатор Интерпола. Ответственность за нарушения и преступления в сфере информационной безопасности. Дисциплинарная ответственность за разглашение охраняемой законом тайны. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации. Уголовная ответственность за преступления в сфере компьютерной информации. Уголовная ответственность за нарушение закона о государственной тайне.

Тема 2. Угрозы безопасности информации

Каналы силового деструктивного воздействия на информацию. Электромагнитный спектр как источник воздействия на информацию. Каналы силового деструктивного воздействия (СДВ) на информацию. Классификация средств СДВ. Рекомендации по защите компьютерных систем от СДВ. Технические каналы утечки информации. Классификация технических каналов утечки информации. Модели и способы утечки информации по техническим каналам.

Угрозы несанкционированного доступа к информации. Классификация угроз несанкционированного доступа (НСД) к информации. Категории нарушителей безопасности информации и их возможности. Общая характеристика уязвимостей. Способы реализации угрозы НСД к информации.

Нетрадиционные информационные каналы. Понятие и обобщенная модель нетрадиционного информационного канала. Методы сокрытия информации в текстовых файлах. Методы сокрытия информации в графических файлах. Методы сокрытия информации в звуковых файлах. Методы сокрытия информации в сетевых пакетах и

исполняемых файлах.

Тема 3. Методы и средства защиты информации от НСД

Криптографическая защита информации. Модель криптосистемы. Историография и классификация шифров. Примеры криптографических алгоритмов. Криптосистема с симметричными и несимметричными ключами. Электронная цифровая подпись.

Методы и средства разграничения и контроля доступа к информации. Мандатная и дискреционная модели доступа. Процедура идентификации, аутентификации и авторизации. Система паролирования. Системы контроля и управления доступом. Система охраны периметра.

Системы предотвращения утечки информации из корпоративной сети. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети. Понятие и функционал DLP-систем. Объем и структура данных защищаемых DLP-системами. Каналы коммуникаций, контролируемые DLP-системами. Критерии оценки программных продуктов, реализующих функциональность DLP.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 3.1

Тема (раздел)	Формы (методы) текущего контроля успеваемости
Тема 1. Нормативная база и стандарты в области информационной безопасности и защиты информации. Компьютерная преступность	Устный опрос, деловая игра «Проблемы и приоритеты в сфере информационной безопасности» / Тестирование
Тема 2. Угрозы безопасности информации	Защита задания/Тестирование
Тема 3 Методы и средства защиты информации от несанкционированного доступа	Круглый стол

4.1.2. Экзамен проводится с применением следующих методов (средств):

Экзамен включает в себя проверку теоретических знаний в форме устного опроса и проверку практических навыков в письменной форме. Во время экзамена проверяется этап освоения компетенций ПКС-1.2.

Во время проверки сформированности этапа компетенции ПКС-1.2 оцениваются:

- выполнение и защита курсовой работы;
- выполнение работ с информационной системой обеспечения информационной безопасности.
- тестирование.

Преподаватель оценивает уровень подготовленности обучающихся к занятию по следующим показателям:

- устные ответы на вопросы преподавателя по теме занятия;
- проверки выполнения домашних заданий;
- по результатам выполнения тестов

Критерии оценивания опроса:

– содержание и формулировки ответов на вопросы;

– полнота и адекватность ответов.

Детализация баллов и критерии оценки текущего контроля успеваемости утверждаются на заседании кафедры.

4. 2. Материалы текущего контроля успеваемости обучающихся.

Материалы текущего контроля успеваемости по ЭК

Типовые оценочные материалы по теме 1

Тест

1. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему (последовательность номеров через запятую):

1) морально-этический;
2) организационно-технический;
3) нормативно-правовой;
4) программно-аппаратный;
5) духовно-нравственный.

2. Что НЕ является элементом системы обеспечения информационной безопасности РФ (номер по порядку)?

1) Палаты Федерального собрания;
2) Президент;
3) Органы местного самоуправления;
4) Общественная Палата;
5) Органы исполнительной власти;
6) Совет безопасности?

3. Кто НЕ наделен полномочиями по отнесению сведений к государственной тайне?

1) Министр сельского хозяйства;
2) Председатель Банка РФ;
3) Руководитель Росгидромета;
4) Руководитель Федеральной таможенной службы?

4. Служба безопасности на предприятии призвана:

1) постепенно заменить государственные правоохранительные органы и специальные службы;
2) помочь олигархическим группам в борьбе за власть;
3) обеспечить безопасность в тех областях, которые находятся вне компетенции правоохранительных органов;
4) осуществлять все, что указано в предыдущих пунктах?

5. Коммерческая тайна – это:

1) общее понятие для тайн профессиональной, личной, семейной;
2) то же самое, что и интеллектуальная собственность;
3) то же самое, что и профессиональная тайна;
4) то же самое, что и банковская тайна;
5) частный случай государственной тайны;
6) частный случай конфиденциальной информации.

6. Основанием для видов коммерческой тайны является:

1) сфера деятельности предприятия;
2) способ организации защиты тайны;
3) отраслевая принадлежность предприятия;
4) все указанное в 1)–3);
5) все указанное в 1)–2).

7. Режим коммерческой тайны не может быть установлен в отношении сведений:

1) о задолженности по выплате зарплаты;
2) о размерах доходов некоммерческих организаций;
3) о составе имущества предприятия любой формы собственности;
4) о системе оплаты труда (неверное зачеркнуть).

8. При отсутствии трудовых договоров охрана КТ должна включать в себя:

1) определение перечня сведений;
2) ограничение доступа;

3) учет лиц, получивших доступ;
4) регулирование отношений с контрагентами;
5) нанесение грифа «Коммерческая тайна» (неверное зачеркнуть).

9. Не подлежит засекречиванию информация о:
1) состоянии окружающей среды;
2) состоянии здоровья премьер-министра;
3) размерах золотовалютного резерва;
4) состоянии борьбы с преступностью;
5) привилегиях.

10. Какой степени секретности НЕ существует:
1) государственной важности;
2) совершенно секретно;
3) особой важности;
4) секретно?

11. Основанием для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:
1) признание его рецидивистом;
2) постоянное проживание близких родственников за границей;
3) сообщение заведомо ложных анкетных данных;
4) наличие медицинских противопоказаний;
5) наличие загранпаспорта (неверное зачеркнуть).

12. К органам защиты государственной тайны относятся:
1) Федеральная служба безопасности;
2) Служба внешней разведки;
3) Министерство внутренних дел;
4) Федеральная служба по техническому и экспортному контролю;
5) Министерство обороны (неверное зачеркнуть).

Ключи:

1	2	3	4	5	6	7	8	9	10	11	12
3),2),4),1),5)	4)	3)	3)	6)	5)	3)	1),2)	4)	1)	5)	3)

Типовые вопросы для опроса

1. Дать понятие компьютерного преступления.
2. Что такое инцидент информационной безопасности?
3. Что положено в основу классификации компьютерных правонарушений?
4. Перечислите и охарактеризуйте преступления, против конфиденциальности, целостности и доступности компьютерных данных и систем.
5. Перечислите и дайте характеристику преступлениям, которые связаны с контентом.
6. Преступления, связанные с правами собственности и товарными знаками. Перечислить и дать характеристику.
7. Преступления, связанные с применением компьютерной техники.
8. Комбинированные преступления.
9. Криминалистическая характеристика правонарушений в компьютерной сфере.

Типовые оценочные материалы по теме 2

Типовые вопросы для опроса по тема 2:

1. Включение кейса с электролитическими конденсаторами в сетевую розетку офисной ЛВС является следующим каналом силового деструктивного воздействия:

1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

2. Включение кейса с электролитическими конденсаторами в офисную розетку сети электропитания является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

3. Включение электрошокера в сетевой разъем маршрутизатора является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

4. Мощный разряд молнии в непосредственной близости является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

5. Внедрение программной закладки в источник бесперебойного питания. является следующим каналом силового деструктивного воздействия:
1) КСДВ – 2;
2) КСДВ – 1;
3) КСДВ – 3.

6. Перехват побочных электромагнитных излучений от работы ПЭВМ и ВТСС является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

7. Съём наводок информационных сигналов с посторонних проводников является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

8. Беспроводной прием информации, передаваемой аппаратными закладками является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

9. Приём переизлученных высокочастотных колебаний, модулированных информационным сигналом является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:
1) электромагнитный;
2) воздушный (акустический);

3) электрический;
4) радиоканал;
5) параметрический.

10. Перехват речевых сигналов направленными микрофонами является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:

1) электромагнитный;
2) воздушный (акустический);
3) электрический;
4) радиоканал;
5) параметрический.

11. По виду защищаемой информации различаются угрозы НСД к:

1) речевой информации;
2) видовой информации;
3) сигнальной информации;
4) логической информации;
5) тестовой информации (лишнее зачеркнуть).

12. По видам возможных источников различаются угрозы НСД к информации, создаваемые:

1) нарушителем;
2) аппаратной закладкой;
3) вредоносными программами;
4) сетевыми атаками (лишнее зачеркнуть).

13. По виду нарушаемого свойства информации различаются угрозы:

1) конфиденциальности;
2) целостности;
3) доступности;
4) идентифицируемости (лишнее зачеркнуть).

26. По способам реализации различаются угрозы с применением:

1) программных средств операционной системы;
2) специально разработанного программного обеспечения;
3) вредоносных программ;
4) пользовательских программ (лишнее зачеркнуть).

14. По используемой уязвимости различаются угрозы:

1) системного программного обеспечения;
2) прикладного программного обеспечения;
3) вызванные аппаратной закладкой;
4) протоколов сетевого взаимодействия;
5) недостатков организации технической защиты информации от НСД;
6) вызванные наличием технических каналов утечки информации;
7) недостатков системы защиты информации:
8) специальных воздействий
(лишнее зачеркнуть)

15. По объекту воздействия различаются угрозы:

1) информации, обрабатываемой на АРМ;
2) информации, обрабатываемой в выделенных технических средствах обработки информации;
3) информации, передаваемой по сетям;
4) прикладным программам обработки информации;
5) системному программному обеспечению;
6) пользовательским программам
(лишнее зачеркнуть)

Ключи:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1)	2)	1)	3)	2)	1)	3)	4)	5)	2)	5)	4)	4)	4)	8)

Типовые оценочные материалы по теме 3

Типовые вопросы для круглого стола

1. По каким схемам можно включить контур информационной безопасности в сеть предприятия?
2. Зачем нужна фильтрация по прокси-серверам?
3. Зачем нужна фильтрация по почтовым серверам?
4. Какие виды поиска рекомендуются для структурированных документов?
5. Что такое фильтр ограничений по перехвату?
6. Что такое «белый список»?
7. Какой должен быть интервал обновления индексов?
8. Для чего применяется каталог образцов?
9. Можно ли снять цифровой отпечаток из pdf-файла?
10. Что такое шаблон регулярного выражения?

4.3. Оценочные средства для промежуточной аттестации.

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Таблица 4.2

Код компетенции	**Наименование компетенции**	**Код этапа освоения индикатора компетенции**	**Наименование компонента компетенции**
ПКС - 1	Способен управлять ресурсами ИТ, инфраструктурой, информационной безопасностью, качеством информационных технологий	ПКС – 1.2	Демонстрирует умения управлять информационной безопасностью ресурсов ИТ, использовать стандарты информационной безопасности, методики и средства обеспечения информационной безопасности

Показатели и критерии оценивания компетенций на различных этапах их формирования

Таблица 4.3

Код компонента компетенции	**Показатель оценивания**	**Критерий оценивания**
ПКС-2.1	Демонстрирует знания основных положений теории информационной безопасности, методов и моделей обеспечения информационной безопасности, в том числе при взаимодействии с партнерами и клиентами. Демонстрирует умение решать частные задачи организации взаимодействия с клиентами и партнерами, управлять информационной безопасностью.	Использует стандарты информационной безопасности, методики управления процессом информационной безопасности Полнота реализации темы курсовой работы.

Для оценки сформированности компетенций, знаний и умений, соответствующих данным компетенциям, используются контрольные вопросы.

Типовые оценочные материалы промежуточной аттестации

Примерная тематика курсовых работ:

1. Защита персональных данных в облачных хранилищах данных.
2. Угрозы безопасности персональным данным при их обработке в информационных системах персональных данных.
3. Риски и вызовы криптовалют для монетарной политики.
4. Правовые аспекты организации обработки персональных данных.
5. Алгоритм шифрования ГОСТ 28147-89.
6. ГОСТ Р 34.10-2012. Процессы формирования и проверки электронной подписи.
7. Защита конфиденциальной информации при работе с лингвистическим анализом DLP- систем.
8. Контроль записи конфиденциальных данных на внешние носители в DLP-системе.
9. Комплексное программное решение для защиты от утечки конфиденциальных данных.
10. Использование цифровых меток для защиты конфиденциальных данных.
11. Использование функции DLP-систем «поиск по атрибутам» при работе с информацией, содержащей конфиденциальные данные.
12. Контроль персональных данных в исходящей электронной почте.
13. Выявление утечки персональных данных с использованием функции DLP-системы «поиск похожих».
14. Использование функции DLP-систем «поиск по словарю» для защиты персональных данных.
15. Контроль информации, содержащей конфиденциальные данные и выводимой на печать.
16. Сложности внедрения DLP-систем для защиты персональных данных.
17. Предотвращение утечки конфиденциальных данных в почтовом трафике на примере программного комплекса SearchInform.
18. Исследование функции фразового поиска DLP-систем при работе с персональными данными.
19. Предотвращение утечек персональных данных путем перехвата содержимого мониторов рабочих станций пользователей.
20. Построение модели комплексной защиты информации на предприятии.
21. Применение запросов с цифровыми отпечатками в DLP-системах при работе с конфиденциальными данными.
22. Оценка необходимости использования «Белых списков» в DLP системах при защите персональных данных.
23. Исследование средств статического анализа уязвимостей.
24. Исследование средств анализа защищенности: сетевые сканеры безопасности.
25. Исследование средств для сбора информации об атакуемой сети.
26. Система защиты государственной тайны в РФ.
27. Порядок допуска сотрудников к государственной тайне.
28. Правовые основы защиты профессиональной тайны в РФ.
29. Каналы утечки электронной конфиденциальной информации.
30. Основные методы защиты электронной конфиденциальной информации.

Вопросы к экзамену по дисциплине «Информационная безопасность»

1) Государственная политика в сфере информационной безопасности и защиты информации.

2) Правовое обеспечение информационной безопасности.
3) Конституция РФ об «информационных правах и обязанностях».
4) Основные нормативные документы, регулирующие отношения в сфере информационной безопасности.
5) Акты регуляторов в сфере защиты информации.
6) Институт «тайны» в Российском законодательстве.
7) Классификация тайн.
8) Правовые основания отнесения сведений к категории ограниченного доступа.
9) Краткая история защиты информации в России.
10) Обобщенная модель информационной безопасности.
11) Институт стандартизации сферы информационной безопасности.
12) Национальные стандарты в области информационной безопасности и защиты информации.
13) Международные стандарты в области информационной безопасности и защиты информации.
14) Проблемы гармонизации стандартов информационной безопасности.
15) «Ландшафт» стандартов информационной безопасности.
16) Электромагнитный спектр как источник воздействия на информацию.
17) Каналы силового деструктивного воздействия (СДВ) на информацию.
18) Рекомендации по защите компьютерных систем от СДВ.
19) Классификация технических каналов утечки информации.
20) Модель и способы утечки по радиоканалу.
21) Модель и способы утечки по электрическому каналу.
22) Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу.
23) Модель и способы утечки по оптическому (оптико-электронному) каналу.
24) Модель и способы утечки по каналу ПЭМИН.
25) Классификация угроз несанкционированного доступа (НСД) к информации.
26) Категории нарушителей безопасности информации и их возможности.
27) Общая характеристика уязвимостей.
28) Способы реализации угрозы НСД к информации.
29) Понятие и обобщенная модель нетрадиционного информационного канала.
30) Методы сокрытия информации в текстовых файлах.
31) Методы сокрытия информации в графических файлах.
32) Методы сокрытия информации в звуковых файлах.
33) Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
34) Историография и классификация шифров.
35) Примеры криптографических алгоритмов.
36) Криптосистема с симметричными и несимметричными ключами.
37) Электронная цифровая подпись.
38) Мандатная и дискреционная модели доступа.
39) Процедура идентификации, аутентификации и авторизации.
40) Система паролирования.
41) Системы контроля и управления доступом.
42) Система охраны периметра.
43) Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
44) Понятие и функционал DLP-систем.
45) Объем и структура данных защищаемых DLP-системами.
46) Каналы коммуникаций, контролируемые DLP-системами.
47) Критерии оценки программных продуктов, реализующих функциональность DLP.

48) Понятие компьютерной преступности.
49) Масштабы и общественная опасность компьютерной преступности.
50) Виды и субъекты компьютерных преступлений.
51) Специфика расследования компьютерных преступлений.
52) Предупреждение компьютерных преступлений.
53) Дисциплинарная ответственность за разглашение охраняемой законом тайны.
54) Административная ответственность за нарушения в сфере информационной безопасности и защиты информации.
55) Уголовная ответственность за преступления в сфере компьютерной информации.

Описание системы оценивания

Оценочные средства (формы текущего и промежуточного контроля)	**Показатели оценки**	**Критерии оценки**
Опрос	Корректность и полнота ответов	**Сложный вопрос:** полный, развернутый, обоснованный ответ – 4 балла Правильный, но не аргументированный ответ – 2 балла Неверный ответ – 0 баллов **Обычный вопрос:** полный, развернутый, обоснованный ответ – 4 балла Правильный, но не аргументированный ответ – 2 балла Неверный ответ – 0 баллов. **Простой вопрос:** Правильный ответ – 2 балла; Неправильный ответ – 0 баллов
Тест	1) Правильность и корректность ответов	В зависимости от семестра максимальное количество баллов за один тес составляет 5 или 10 баллов
Защита задания	1) полнота раскрытия темы; 2) представляемая информация систематизирована и логически связана; 3) даны ответы на все вопросы; 4) выполнена презентация	При условии 2-х заданий в семестре, максимальное количество баллов за каждую из них – 10.

Оценивание студентов на экзамене по дисциплине «Информационная безопасность»

Баллы %	**Критерии**
100-85 «отлично»	Оценка «отлично» на экзамене выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое

	решение.
84-61 «хорошо»	– Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения, допускает неточности в увязывании теории с практикой.
60-51 «удовлетворительно»	– Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при установлении связи теории и практики.
Менее 51 «неудовлетворительно»	– Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями устанавливает связь теории и практики.

Шкала оценивания.

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Схема расчетов сформирована в соответствии с учебным планом направления, согласована с руководителем научно-образовательного направления, утверждена деканом факультета. Схема расчетов доводится до сведения студентов на первом занятии по данной дисциплине и является составной частью рабочей программы дисциплины и содержит информацию по изучению дисциплины, указанную в Положении о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС.

На основании п. 14 Положения о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС в институте принята следующая шкала перевода оценки из многобалльной системы в пятибалльную:

Таблица 4.4

Количество баллов	**Экзаменационная оценка**	
	прописью	буквой
96 - 100	отлично	A
86 - 95	отлично	B
71 - 85	хорошо	C
61 - 70	хорошо	D
51 – 60	удовлетворительно	E
0 - 50	неудовлетворительно	EX

Шкала перевода оценки из многобалльной в систему «зачтено»/ «не зачтено»:

Таблица 4.5

от 0 до 50 баллов	«не зачтено»
от 51 до 100 баллов	«зачтено»

Примечание: если дисциплина изучается в течение нескольких семестров, схема расчета приводится для каждого из них.

4.4. Методические материалы по освоению дисциплины

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, включают в себя:

- комплект тестовых заданий по темам дисциплины,
- рекомендации и требования к выполнению и оформлению курсовых работ,

– критерии оценивания курсовых работ,

– требования к защите курсовых работ и критерии их оценивания,

– основания для получения максимального количества баллов по защите курсовой работы,

– основания для снижения количества баллов в диапазоне от max до min по защите курсовой работы,

– указания причин для доработки курсовой работы и допуска к экзамену по дисциплине. Методические материалы в виде презентаций размещены в Ресурсах сети СЗИУ в STUDBOX в папке кафедры.

5. Методические указания для обучающихся по освоению дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия, курсовые работы. Преподавание дисциплины ведется с применением следующих видов образовательных технологий, обусловливающих самоорганизацию процесса освоения дисциплины.

Организация работы с информацией.

Информационные технологии: обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки и объективного контроля и мониторинга знаний студентов.

Использование электронных образовательных ресурсов (презентационный материал, размещенный в Ресурсах сети СЗИУ) при подготовке к лекциям, практическим занятиям. Организация работы студентов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

Проблемное обучение (проблемные лекции, лекции с элементами дискуссии) с целью развитие критического мышления, стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы. Для этого студенту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет.

Развитие профессиональной компетентности:

Case-study на практических занятиях с целью формирования способности к анализу реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.

Контекстное обучение (лекции с элементами дискуссии, практические занятия) с целью развития мотивации бакалавров к усвоению знаний путем выявления связей между конкретным знанием и его применением.

Организация группового взаимодействия в образовательном процессе.

Деловая игра: на практических занятиях ролевая имитация студентами реальной профессиональной деятельности с выполнением функций специалистов на различных рабочих местах, организация дискуссии, обучения на основе социального взаимодействия.

Работа в команде с целью развития способности к взаимодействию студентов в группе при выполнении домашних заданий по разделам дисциплины.

Осуществление учения с учетом возрастающей роли субъектности и самостоятельности:

Обучение на основе опыта: активизация познавательной деятельности студентов за счет ассоциации и собственного опыта с предметом изучения, самоуправляемого обучения, самообразовательной деятельности

С целью контроля сформированности компетенций разработан фонд контрольных заданий.

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 следующем:

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

Подготовка к семинарским занятиям:

- внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
- выпишите основные термины;
- 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.

Подготовка к экзамену.

К экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- контрольными мероприятиями;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к экзамену.

После этого у вас должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и семинарских занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР :

ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 10.07.2024). – Режим доступа: по подписке.

2. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 10.07.2024). – Режим доступа: по подписке.

3. 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.

4. 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.

5. Попов, И. В. Информационная безопасность: практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 10.07.2024). – Режим доступа: по подписке.

6. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/467370.

7. Попов, И. В. Информационная безопасность: практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 10.07.2024). – Режим доступа: по подписке.

8. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/475890.

9. 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.

6.2 Дополнительная литература

1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. —

243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/476294.

6.3. Нормативные правовые документы.

Не используются

6.4. Интернет-ресурсы.

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

Русскоязычные ресурсы

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

Электронные учебники электронно - библиотечной системы (ЭБС) «Юрайт».

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

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

Рекомендуется использовать следующий интернет-ресурсы.

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

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

6.5. Иные источники.

Не используются.

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

Практические занятия проводится в компьютерном классе. Учебная дисциплина включает использование программного обеспечения Microsoft Excel, Microsoft Word, 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).

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
2.	Пакет Excel -2013, 2017, proffesional plus
3.	Мультимедийные средства в каждом кмпьютерном классе и в лекционной аудитории
4.	Браузер, сетевые коммуникационные средства для выхода в Интернет
5.	Поисковая правовая система «Консультант +»

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.