МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
Код и наименование направления подготовки

Организация и технологии защиты государственной тайны
Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Технологии обеспечения информационной безопасности
Рабочая программа дисциплины

Составитель:
к.т.н, доцент, доцент, Н.В. Гришина

Ответственный редактор
к.и.н., доцент, заведующая кафедрой, Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 30.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: формирование у обучающихся знаний в области технологий обеспечения информационной безопасности; изучение и освоение основных технологий, используемых при формировании системы защиты информации предприятия.

Задачи дисциплины: анализ основных видов технологий обеспечения безопасности; изучение и освоение состава подсистем системы защиты информации, особенностей их создания и внедрения.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения	Знать: типовую структуру системы защиты информации; методики анализа результатов исследования; Уметь: разрабатывать стратегию проведения исследований; анализировать структуру систем защиты информации; Владеть: опытом организации процесса принятия решения
	УК-1.2. Умеет принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий	Знать: методики разработки стратегий действий при проблемных ситуациях; Уметь: принимать конкретные решения для повышения эффективности процедур анализа проблем Владеть: опытом применения полученных знаний в научно-исследовательской и практической работе;
	УК-1.3. Владеет методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях	Знать: методики постановки цели и определения способов ее достижения; Уметь: пользоваться методами установления причинно-следственных связей и определения наиболее значимых среди них; Владеть: методиками постановки цели и определения способов ее достижения;
ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1. Знать основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности	Знать: основные национальные и зарубежные стандарты в области обеспечения информационной безопасности; Уметь: работать со стандартами и нормативными документами в своей профессиональной деятельности; Владеть: навыками использования международных и национальных стандартов в области информационной безопасности;
	ОПК-1.2. Уметь	Знать: основные этапы проектирования

	проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности	систем защиты информации; Уметь: проектировать системы защиты информации с использованием различных технологий обеспечения информационной безопасности; Владеть: навыками проектирования системы защиты информации
	ОПК-1.3. Владеть навыками участия в разработке системы обеспечения информационной безопасности объекта	Знать: основные разделы технического задания на проектирование системы защиты информации; Уметь: пользоваться приобретёнными знаниями для формирования проекта технического задания на создание системы защиты информации; Владеть: навыками участия в разработке системы защиты информации объекта
ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компоненты системы) обеспечения информационной безопасности	ОПК-2.1. Знает методы концептуального проектирования технологий обеспечения информационной безопасности	Знать: методы концептуального проектирования технологий обеспечения информационной безопасности; Уметь: работать в команде с целью разработки технического проекта системы обеспечения информационной безопасности; Владеть: методами концептуального проектирования технологий обеспечения информационной безопасности;
	ОПК-2.2. Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	Знать: методы решения задач для защиты информации в системах и информационно-коммуникационных сетях; Уметь: выбирать и обосновывать преимущества методов решения задач для защиты информации в системах и информационно-коммуникационных сетях; Владеть: навыками решения задач для защиты информации в системах и информационно-коммуникационных сетях;
	ОПК-2.3. Владеет навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	Знать: структуру технического проекта системы обеспечения информационной безопасности; Уметь: выбирать соответствующие технологии обеспечения информационной безопасности при разработке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности; Владеть: навыками выполнения работы при наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Технологии обеспечения информационной безопасности» относится к базовой части блока дисциплин учебного плана, изучается в 2-ом семестре.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующей дисциплины: "Защищенные информационные системы".

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: "Технологии защиты информации в компьютерных сетях", "Технология построения защищенных систем обработки информации".

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 академических часа

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	32
2	Практические работы	44
	Всего:	76

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 68 академических часа.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Требования к технологии управления информационной безопасностью. Основные принципы реализации технологий обеспечения безопасности	Предмет и содержание дисциплины, основные понятия, методы изучения, основная литература, контроль освоения дисциплины. Основные стадии развития средств и методов защиты информации. Типовая структура системы защиты информации. Базовые требования к технологии управления информационной безопасностью. Основные принципы реализации технологий обеспечения безопасности.
2	Основные виды технологий обеспечения информационной безопасности	Особенности IPS-систем по выявлению и предотвращению вторжений. Роль межсетевого экранирования и основные классы межсетевых экранов. Защита от компьютерных вирусов. Идентификация и аутентификация пользователей и основные используемые при этом технологии. Основные методы реализации доступа к информации.

		Особенности криптографической защиты информации. Назначение DLP-систем.
3	Структура и состав подсистем системы защиты информации	Основные функциональные и обеспечивающие подсистемы системы защиты информации. Назначение функциональных и обеспечивающих подсистем. Классификация автоматизированных систем с учётом обеспечения информационной безопасности и требования по защите информации. Основные функциональные подсистемы и требования по уровню защищённости, предъявляемые к ним.
4	Проектирование и внедрение системы защиты информации	Основные этапы разработки системы защиты информации. Назначение и структура технического задания на систему. Состав технического и рабочего проектов. Особенности внедрения системы защиты информации.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Требования к технологии управления информационной безопасностью. Основные принципы реализации технологий обеспечения безопасности	Лекция 1	Вводная лекция с использованием видеопроектора
		Практическое занятие 1	опрос
		Самостоятельная работа	Подготовка к занятию с использованием электронного курса лекций
2.	Основные виды технологий обеспечения информационной безопасности	Лекция 2	Лекция с использованием видеопроектора
		Практическое занятие 2	опрос
		Самостоятельная работа	Подготовка к занятию с использованием электронного курса лекций
3.	Структура и состав подсистем системы защиты информации	Лекция 3	Лекция с использованием видеопроектора
		Практическое занятие 3	опрос
		Самостоятельная работа	Подготовка к занятию с использованием электронного курса лекций
4.	Проектирование и внедрение системы защиты информации	Лекция 4	Лекция с использованием видеопроектора
		Практическое занятие 4	опрос
		Контрольная работа	Подготовка к контрольной с использованием электронного курса лекций
		Самостоятельная	Подготовка к занятию с

		работа	использованием электронного курса лекций

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос или тестирование* *- контрольная работа (темы 3-4)*	 *10 баллов* *20 баллов*	 *40 баллов* *20 баллов*
Промежуточная аттестация *(зачёт с оценкой по билетам)*		*40 баллов*
Итого за семестр *зачёт с оценкой*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	**Традиционная шкала**		**Шкала ECTS**
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценок

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A, B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой,

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	удовлетворительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	неудовлетворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Примерные вопросы к опросу

1. Понятия информационной безопасности и защиты информации.
2. Охарактеризуйте эпоху Интернет-2 в России.
3. Основные аспекты, учитываемые при вводе в эксплуатацию DLP-систем.
4. Понятие технологии обеспечения информационной безопасности.
5. Основные способы аутентификации.
6. Базовые методы несанкционированного доступа к информации.
7. Обеспечивающие подсистемы системы защиты информации (СЗИ).
8. Основные виды технологий обеспечения информационной безопасности.

Примерные вопросы к тестированию (открытый вопрос)
(проверка сформированности компетенции УК-1):

1. Какой документ определяет перечень сведений конфиденциального характера?
2. Принцип рассмотрения проекта, при котором анализируется система в целом, а не ее отдельные части – это...
3. Какая главная цель системы менеджмента информационной безопасности?
4. Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?
5. Какой орган осуществляет контроль за обеспечением защиты сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях; в установленном порядке осуществляет мероприятия, связанные с допуском граждан к сведениям, составляющим государственную тайну:
6. Какая организация осуществляет организацию и обеспечение эксплуатации, безопасности, развития и совершенствования правительственной связи, иных видов специальной связи и систем специальной информации для государственных органов; обеспечение в пределах своей компетенции сохранности государственных секретов; организация и обеспечение криптографической и инженерно-технической безопасности шифрованной связи в Российской Федерации и ее учреждениях за рубежом; лицензирование деятельности в области криптографической защиты информации и сертификация криптографических средств защиты:
7. Ответственность за организацию защиты сведений, составляющих государственную тайну в органах государственной власти на предприятиях, в учреждениях и организациях, возлагается на …
8. Высшая степень защиты сведений, составляющих государственную тайну, имеет гриф …:
9. Совокупностью каких групп систем может быть представлено множество компонентов, составляющих объект информатизации?

-люди (биосоциальные системы)

-техника (технические системы и помещения, в которых они расположены)

- программное обеспечение, которое является интеллектуальным посредником между человеком и техникой (интеллектуальные системы)

10. Значимость комплексного подхода к организации защиты информации состоит:

-в объединении локальных систем защиты

- в обеспечении полноты всех составляющих системы защиты

-в обеспечении всеохватности защиты информации

Примерные вопросы к тестированию (открытый вопрос)
(проверка сформированности компетенции ОПК-1):

1. Какой ГОСТ Р содержит свод норм и правил применения мер обеспечения информационной безопасности?
2. Определите соответствие между понятиями:

Идентификация – процедура, в результате выполнения которой для субъекта выявляется его уникальный признак, однозначно определяющий его в информационной системе.

Аутентификация – процедура проверки подлинности, например, проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

Авторизация – предоставление определенному лицу прав на выполнение определенных действий

3. Что такое эффективность защиты информации?
4. Кто устанавливает политику информационной безопасности компании?
5. В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам - это
6. Определите соответствие между определением стратегии защиты информации и содержанием:

оборонительная — защита от уже известных угроз, осуществляемая автономно, т. е. без оказания существенного влияния на информационно-управляющую систему;

наступательная — защита от всего множества потенциально возможных угроз, при осуществлении которой в архитектуре информационно-управляющей системы и технологии ее функционирования должны учитываться условия, продиктованные потребностями защиты;

упреждающая — создание информационной среды, в которой угрозы информации не имели бы условий для проявления

7. Как определяется в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" конфиденциальность информации?
8. Как определяется в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" распространение информации?
9. Может ли быть ограничен доступ к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления?

10. Какой орган исполнительной власти наделен полномочием выдавать лицензии на деятельность по созданию средств защиты информации, предназначенные для защиты (сохранения) государственной тайны?:
11. В соответствии с комплексным (системным) подходом приступать к созданию системы защиты информации можно, когда определены следующие ее компоненты:

Примерные вопросы к тестированию (открытый вопрос)
(проверка сформированности компетенции ОПК-2):

1. При создании систем защиты информации рекомендуется выделять следующие этапы:
2. Определите соответствие между понятиями:

Открытый ключ - позволяет проверить электронную подпись под документом
Закрытый ключ - нужен для создания электронной подписи

3. Определите соответствие типа управленческих решений:

– организационные – предусматривают формирование новой или совершенствование имеющейся структуры управления компанией, а также комплекс административных мероприятий по организации выполнения задания;
– координирующие – при появлении непредвиденных в плане мешающих воздействий необходимы для гармонизации деятельности компании;
– контролирующие решения направлены на обеспечение своевременного выполнения планов и намеченных рубежей развития

4. К какому типу мер обеспечения безопасности относится установка межсетевого экрана?
5. Для чего используется электронная подпись?
6. Принципы, в соответствии с которыми строится система защиты информации:
7. Как можно определить систему предотвращения вторжений?
8. Определите основную функцию межсетевого экрана
9. Соотнесите форму реализации управленческого решения и ее содержание

Сообщение – деловая беседа, проводимая руководителем с целью передачи дополнительной информации, необходимой для выполнения управленческих решений.
Личный пример – действия руководителя в среде подчиненных по заранее подготовленному сценарию для развития у них эффекта подражания авторитетам в технике выполнения управленческих решений.
Обучение – деловая беседа, проводимая руководителем с целью дать новые знания или информацию для выполнения управленческих решений.

10. Что нужно знать для передачи сообщений с помощью симметричных алгоритмов шифрования?
11. Соотнесите формы подготовки и реализации управленческих решений

формы подготовки -- указ, закон, приказ, распоряжение, указание
формы реализации-- предписание, убеждение

Примерная тематика контрольной работы

1. Структура системы защиты информации.
2. Базовые требования к технологии управления информационной безопасностью.
3. Основные задачи, решаемые DLP-системами.
4. Отличительные свойства биометрических идентификаторов.

5. Динамические и статические биометрические идентификаторы.
6. Классификация систем обнаружения вторжений.
7. Симметричные и ассиметричные методы шифрования.
8. Основные классы автоматизированных систем с учётом требований по их защите.
9. Базовые требования к подсистеме управления доступом СЗИ.
10. Структура технического проекта СЗИ.
11. Основные требования к подсистеме регистрации и учёта СЗИ.
12. Классификация межсетевых экранов.

Промежуточная аттестация

Примерная тематика вопросов для зачёта с оценкой

1. Основные этапы развития методов и средств защиты информации в процессе эволюции человечества.
2. Базовые элементы типовой системы защиты информации (СЗИ).
3. Основные принципы реализации технологий обеспечения безопасности.
4. Характеристика DLP-систем, представленных на российском рынке.
5. Основные методы реализации доступа к информации.
6. Базовые задачи, решаемые межсетевыми экранами.
7. Особенности биометрической системы защиты информации.
8. Основные алгоритмы криптографической защиты информации.
9. Функциональные подсистемы системы защиты информации.
10. Основные требования к криптографической подсистеме СЗИ.
11. Основные требования к подсистеме обеспечения целостности СЗИ.
12. Характеристика современных IPS-систем по обнаружению и предотвращению вторжений.
13. Характеристика антивирусных программных комплексов на российском рынке.
14. Основные стадии проектирования системы защиты информации.
15. Базовые разделы технического задания на СЗИ.
16. Особенности внедрения СЗИ.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

ГОСТ Р 59339-2021 Национальный стандарт Российской Федерации. Системная инженерия. Защита информации в процессе управления рисками для системы

ГОСТ Р 58771-2019 Национальный стандарт Российской Федерации. Менеджмент риска Технологии оценки риска

ГОСТ Р ИСО 31000-2019 Национальный стандарт Российской Федерации. Менеджмент риска принципы и руководство

Литература

Основная

Баранов В.В., Горошко И.В., Торопов Б.А., Лебедев В.Н., Петрова В.Ю., Макаров В.Ф. Информационные технологии управления и организация защиты информации

(учебное пособие) - М.: Академия управления МВД России, 2018. - 456 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=44544096

Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации (учебное пособие). СПб: Национальный исследовательский университет ИТМО, 2018. - 100 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=44449457

Кияев В.И., Саитов А.В. Комплексная информационная безопасность в управлении современным предприятием (учебное пособие). СПб. : Изд-во СПбГЭУ, 2016. – 222 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=27189328

Дополнительная

Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации (учебное пособие) - М.: РИОР, ИНФРА-М, 2016. - 322 с. - Режим доступа: URL: https://znanium.com/read?id=217551

Журилова Е.Е., Шабуров А.С. О нормативно-правовых аспектах внедрения DLP-систем // Вестник УрФО. Безопасность в информационной сфере. 2015. - № 3(17). - С. 37-41. - Режим доступа: URL: https://elibrary.ru/item.asp?id=25360156

6.2. Перечень ресурсов информационно-телекоммуникационной сети Интернет

Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru

Национальный открытый университет ИНТУИТ. - Режим доступа: URL: http://www.intuit.ru

Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru

6.3. Перечень современных профессиональных баз данных и информационно-справочных систем

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
Консультант Плюс
Гарант

7. Материально-техническое обеспечение дисциплины

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащён Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Состав программного обеспечения (ПО)

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно*

			***распространяемое*)**
1.	Adobe Master Collection CS4	Adobe	лицензионное
2.	Microsoft Office 2010	Microsoft	лицензионное
3.	Windows 7 Pro	Microsoft	лицензионное
4.	Kaspersky Endpoint Security	Kaspersky	лицензионное
5.	Zoom	Zoom	лицензионное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Тема 1. Типовая структура системы защиты информации

Задания:

1. Понятие системы защиты информации.
2. Постройте иерархическую систему из понятий "компьютерная безопасность", "защита данных", "информационная безопасность", "информация".
3. Основные элементы системы защиты информации (СЗИ)
4. Содержание элемента СЗИ "Правовая защита информации".
5. Методы, реализуемые в организационной защите информации при создании СЗИ.
6. Особенности страховой защиты информации.
7. Средства и методы, реализуемые при использовании криптографической защиты информации.
8. Сущность психологической защиты информации.

Тема 2. Биометрическая аутентификация как современный рубеж защиты информации

Задания:

1. Понятия идентификации и аутентификации.
2. Основные способы аутентификации.
3. Причины широкого распространения в наши дни биометрических технологий защиты информации.

4. Классификация биометрических идентификаторов.
5. Базовые свойства биометрических идентификаторов.
6. Основные цели реализации биометрических технологий защиты информации.
7. Базовые группы защиты биометрических систем от муляжей биометрических идентификаторов.
8. Основные пути повышения эффективности систем биометрической идентификации.

Тема 3. Особенности функциональных подсистем системы защиты информации

Задания:

1. Основные принципы достижения архитектурной безопасности СЗИ.
2. Понятие функциональной подсистемы СЗИ.
3. Основные группы СЗИ, различающиеся требованиями к уровню защиты.
4. Классификация СЗИ с учётом требований по её защите..
5. Основные требования по защите к подсистеме регистрации и учёта .
6. Особенности подсистемы управления доступом СЗИ.
7. Основные требования по защите к подсистеме обеспечения целостности.
8. Особенности криптографической подсистемы СЗИ.

Тема 4. Разработка технического проекта системы защиты информации

Задания:

1. Структура технического проекта СЗИ.
2. Особенности раздела постановки задач и алгоритмов их решения.
3. Содержание организационного обеспечения СЗИ
4. Особенности технического обеспечения СЗИ.
5. Содержание информационного обеспечения СЗИ.
6. Особенности программного обеспечения СЗИ.
7. Содержание раздела "Расчёт экономической эффективности СЗИ".
8. Структура раздела "Мероприятия по подготовке СЗИ к внедрению".

Приложени1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: формирование у обучающихся знаний в области технологий обеспечения информационной безопасности; изучение и освоение основных технологий, используемых при формировании системы защиты информации предприятия.

Задачи дисциплины: анализ основных видов технологий обеспечения безопасности; изучение и освоение состава подсистем системы защиты информации, особенностей их создания и внедрения.

Дисциплина направлена на формирование следующих компетенций:

- УК-1. Способен проводить систематизацию, алгоритмизацию конкретных информационных потоков по месту научных исследований, производственной деятельности;
- ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;
- ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компоненты системы) обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен:

Знать: типовую структуру системы защиты информации; методики анализа результатов исследования; методики разработки стратегий действий при проблемных ситуациях; основные национальные и зарубежные стандарты в области обеспечения информационной безопасности; методики постановки цели и определения способов ее достижения; основные этапы проектирования систем защиты информации; основные разделы технического задания на проектирование системы защиты информации; методы концептуального проектирования технологий обеспечения информационной безопасности; методы решения задач для защиты информации в системах и информационно-коммуникационных сетях; структуру технического проекта системы обеспечения информационной безопасности;

Уметь: разрабатывать стратегию проведения исследований, анализировать структуру систем защиты информации; принимать конкретные решения для повышения эффективности процедур анализа проблем; пользоваться методами установления причинно-следственных связей и определения наиболее значимых среди них; работать со стандартами и нормативными документами в своей профессиональной деятельности; проектировать системы защиты информации с использованием различных технологий обеспечения информационной безопасности; пользоваться приобретёнными знаниями для формирования проекта технического задания на создание системы защиты информации; работать в команде с целью разработки технического проекта системы обеспечения информационной безопасности; выбирать и обосновывать преимущества методов решения задач для защиты информации в системах и информационно-коммуникационных сетях; выбирать соответствующие технологии обеспечения информационной безопасности при разработке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности;

Владеть: опытом организации процесса принятия решения; методиками постановки цели и определения способов ее достижения; опытом применения полученных знаний в научно-исследовательской и практической работе; навыками использования международных и национальных стандартов в области информационной безопасности; навыками проектирования системы защиты информации; навыками участия в разработке системы защиты информации объекта; методами концептуального проектирования технологий обеспечения информационной безопасности; навыками решения задач для защиты информации в системах и информационно-коммуникационных сетях; навыками выполнения работы при наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлена основная литература*	17.03.2023	***9***

Приложение 1
к листу изменений

Обновление основной литературы (2023 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:
1. Дополнить раздел **Основная литература**

Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2023. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1915704 (дата обращения: 22.07.2023).

Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 216 с. - ISBN 978-5-16-016719-0. - Текст: электронный. - URL: https://znanium.com/catalog/product/1900721

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, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657

Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912992

Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912987

Составитель:
К.т.н., доцент, доцент, Н.В.Гришина