Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Костровец Лариса Борисовна
Должность: директор
Дата подписания: 21.10.2026 12:13:22
Уникальный программный ключ:
6882606104c36dbde41c4ab93a65382136a292d6

Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.02.13 Технологии обеспечения информационной безопасности
(индекс, наименование дисциплины в соответствии с учебным планом)

09.03.03 Прикладная информатика
(код, наименование направления подготовки/специальности)

Прикладная информатика в управлении корпоративными информационными системами
(наименование образовательной программы)

Очная форма обучения
(форма обучения)

Год набора – 2026
Донецк

Автор(ы)-составитель(и) РПД:

Семичастный Игорь Леонидович, доцент кафедры информационных технологий

Заведующий кафедрой:

Брадул Наталья Валерьевна, канд. физ.-мат. наук, заведующий кафедрой информационных технологий

Рабочая программа дисциплины Б1.О.02.13 Технологии обеспечения информационной безопасности одобрена на заседании кафедры информационных технологий факультета государственной службы и управления Донецкого филиала РАНХиГС.

Протокол № 7 от «05» марта 2026 г.

СОДЕРЖАНИЕ

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

2. Объем и место дисциплины в структуре образовательной программы

3. Содержание и структура дисциплины

4. Типы оценочных материалов, показатели и критерии их оценивания

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

7. Методические материалы по освоению дисциплины

8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

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

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

Дисциплина Б1.О.02.13 Технологии обеспечения информационной безопасности обеспечивает формирование у обучающихся следующих общепрофессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС *(при наличии)* **	**Код компетенции ****	**Наименование Компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
-	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает** основы информационной культуры и требования информационной безопасности. **Умеет** применять информационно-коммуникационные технологии с учетом требований информационной безопасности.

** Дисциплина может формировать компетенцию полностью или частично.*
***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Общий объем дисциплины:

2,00 з.е., 72 ак.час

Контактная работа обучающихся с преподавателем по видам учебных занятий: 40 ак. час на контактную работу с преподавателем, из них 18 ак. час на лекции и 18 ак. час на практические занятия, 4 часов на Каттэк. 32 ак. час на самостоятельную работу обучающихся.

Б1.О.02.13 Технологии обеспечения информационной безопасности реализуется в 5-м семестре 3-го курса после изучения дисциплин:

- ИТ инфраструктура предприятия;
- Корпоративные информационные системы.

.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
РАЗДЕЛ 1. ТЕХНОЛОГИИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИБ															
Тема 1.1	Основные понятия ИБ. ИБ в системе национальной безопасности России. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	7	2	0	0	4	0	0	0	0		0	0	1	Контрольные вопросы, практические занятия, КТ1

Тема 1.2	Угрозы информационной безопасности. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	5	2	0	0	0	0	0	0	0		0	0	3	Контрольные вопросы, практические занятия, КТ1
Тема 1.3	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	5	2											3	Контрольные вопросы, практические занятия, КТ1
Тема 1.4	Технологии защиты от вредоносных программ и спама. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.	11	2			4								5	Контрольные вопросы, практические занятия, КТ1
РАЗДЕЛ 2. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ															

Тема 2.1	Основные принципы и методы в области технической защиты информации.	11	2	0	0	4	0	0	0	0		0	0	5	Контрольные вопросы, практические занятия, КТ2
Тема 2.2	Противодействие несанкционированному доступу к конфиденциальной информации/ Социальная инженерия	7	2	0	0		0	0	0	0		0	0	5	Контрольные вопросы, практические занятия, КТ2
Тема 2.3	Классификация криптографических методов защиты. Симметричные криптографические алгоритмы	11	2			4								5	Контрольные вопросы, практические занятия, КТ2
Тема 2.4	Асимметричные криптографические алгоритмы	6	2	0	0		0	0	0	0		0	0	4	Контрольные вопросы, практические занятия, КТ2

Тема 2.5	Цифровая электронная подпись (ЭЦП). Технологии аутентификации.	9	2	0	0	2	0	0	0	4		0	0	1	Контрольные вопросы, практические занятия, КТ2
Промежуточная аттестация		**72**	**18**	**0**	**0**	**18**	**0**		**0**	**4**	**0**	**0**	**0**	**32**	**Зачет**
Итого		**72**	**18**	**0**		**18**	**0**		**0**	**4**	**0**	**9**	**0**	**32**	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

РАЗДЕЛ 1. ТЕХНОЛОГИИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИБ

Тема 1.1 Основные понятия ИБ. ИБ в системе национальной безопасности России. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба. ОПК-3.1

Содержание лекции: Введение в информационную безопасность. Ситуация с ИБ в РФ. Понятие информационного объекта, свойства информации как объекта. Информационное общество, шестой технологический и экономический уклад как результат объективного процесса смены укладов. Информационное пространство и его компоненты, информационное взаимодействие. Геополитическая эволюция развития человечества. Принципы, действующие в информационном пространстве. Ключевые характеристики современного информационного общества. Ситуация в России и мире сточки зрения угроз ИБ**.** Основные понятия, термины и определения в области информационной безопасности. Понятие информационной безопасности: конфиденциальность, целостность и доступность информации. Нормативно-правовое регулирование ИБ в РФ. Доктрина информационной безопасности Российской Федерации

Практическая подготовка: Требования по созданию надежных паролей. Применение программы генерации паролей Advanced Password Generator (https://drive.google.com/open?id=1Q7qLTrCefuZNJ3XDzq0FFZ2lWIsINW-S). Генерация при помощи скачанной программы группы паролей по следующей схеме: 8-9(10)-12-20 символов (буквы / буквы+цифры / буквы+цифры+спецсимволы). При помощи интернет ресурсов https://bitwarden.com/password-strength/, https://2ip.ru/passcheck/ и https://password.kaspersky.com/ru/ проверить сгенерированные пароли. Описать изменения стойкости паролей в зависимости от их структуры (описания подтвердить скриншотами). Создать на основе изученных Вами правил надежный пароль уровня Strong. Записать его и использовать в данной работе. Изучить программный продукт хранения паролей KeePass, скачав его с интернет-ресурса https://keepass.info/, установить программу KeePass и создайть свою базу данных паролей. Ознакомится с работой генератора паролей. Воспользуйтесь генератором для создания мастер- пароля. Создать свою портативную базу паролей на сменном носителе. Создать новую базу паролей. Добавить записи о пароле в базу. Добавить в свою базу все пароли: для почты, соцсетей и другие пароли. Создать резервную копию базы паролей, сохранить ее на сменном носителе. Ознакомиться с работой сервиса хранения паролей LastPass (https://www.lastpass.com/ru). Описать его сильные и слабые стороны в сравнении с KeePass, обосновать свои выводы

Тема 1.2. Угрозы информационной безопасности. Политика безопасности и формирование организационной структуры системы

защиты информации на предприятии. ОПК-3.1

Содержание лекции: компоненты модели информационной безопасности на первом уровне декомпозиции. Общая классификация угроз ИБ. Уязвимость основных структурно-функциональных элементов распределенных ИС. Классификация угроз ИБ. Классификация каналов проникновения в систему и утечки информации: физический, электромагнитный, программно-математический. Проблемы безопасности IP-сетей. Виды атак. Подслушивание (sniffing). Изменение данных. Анализ сетевого трафика. Подмена доверенного субъекта. Spoofing. Посредничество в обмене незашифрованными ключами (атака man-in-the-middle). Перехват сеанса (session hijacking). Отказ в обслуживании (Denial of Service, DoS). DDoS-атака. Методы защиты от DDoS атак. Парольные атаки. Метод полного перебора (brute force attack). Угадывание ключа. Атаки на уровне приложений. Злоупотребление доверием. Компьютерные вирусы, сетевые «черви», программа «троянский конь». Рекомендации по обеспечению информационной безопасности предприятия.

Практическая подготовка: Скачать программу Anvide Seal Folder. Изучить возможности программы Anvide Seal Folder. Создайте на домашнем ПК папку, не видимую другим пользователям, защищенную паролем. Используйте для доступа к этой папке созданный пароль. Скачать программу VeraCrypt. Изучить возможности программы VeraCrypt. Создать на ПК небольшой криптоконтейнер, использовав для этого флешку. Используйте для доступа к этому диску созданный пароль. Изучить возможности программы Windows Bitlocker. Используя программу Windows Bitlocker, создайте на ПК небольшой зашифрованный диск. Используйте для доступа к этому диску созданный пароль. Сравнить все опробованные программы, укажите их слабые и сильные стороны, а также функциональные особенности. Сделать выводы о целесообразности применения той или иной рассмотренной программы в определенных условиях (офис, домашнее использование, сменный носитель информации). Отразить выполненные задания в отчете-презентации и используйте ее при защите отчета данной Практической работе.

Тема 1.3 Политика безопасности и формирование организационной структуры системы защиты информации на предприятии. ОПК-3.1

Содержание лекции: Основные типы политики безопасности. Два подхода в обеспечении ИБ в организации. Законодательные меры обеспечения ИБ. Доктрина информационной безопасности. Уголовный кодекс РФ. Различные виды тайн: Закон РФ от 21.07.1993 N 5485- «ЗАКОН О ГОСУДАРСТВЕННОЙ ТАЙНЕ». Законы регуляторов в области ИБ. Политика безопасности в организации. истема обеспечения информационной безопасности (СОИБ). Требования к политике безопасности ИС. Анализ, задание и контроль требований к безопасности. Ключевые средства контроля безопасности ИС. Основные понятия политики безопасности. Структура политики безопасности

организации.

Практическая подготовка: Загрузить ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3. «Методы менеджмента безопасности информационных технологий». Ознакомиться с Федеральным законом от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Ознакомьтесь с Приложениями C, D и E ГОСТа. Выбрать три различных информационных актива организации (см. вариант индивидуального задания). По каждому активу дать наименование, описание, условную стоимость в рублях. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов. Пользуясь Приложением C ГОСТа, сформулируйте три угрозы, реализация которых возможна, пока в системе не устранены названные в пункте 4 уязвимости. Сформулируйте модель или модели нарушителя для этих угроз. Пользуясь двумя методами (см. вариант) предложенных в Приложении E ГОСТа, произведите оценку рисков информационной безопасности. Рассчитать экономические потери от реализации угроз (количественный оценки рисков): по каждой угрозе; в сумме для организации. Разработать систему защитных мер по обеспечению безопасности, которые должны блокировать угрозы. При этом расставить приоритеты, в соответствии с выполненным ранжированием угроз. Разработать политику безопасности, которая является системой управления информационной безопасностью Вашего предприятия. В ее основе перечень вопросов для предприятия (на примере Приложения A ГОСта).

Тема 1.4 Технологии защиты от вредоносных программ и спама. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. ОПК-3.1

Содержание лекции: Классификация вредоносных программ. Основы работы антивирусных программ. Сигнатурный анализ. Особенности «облачной» антивирусной технологии. Проактивные методы обнаружения. Дополнительные модули. Режимы работы антивирусов. Антивирусные комплексы. Дополнительные средства защиты. Брандмауэры. Средства защиты от нежелательной корреспонденции. Защита персональных компьютеров и корпоративных систем от воздействия вредоносных программ и вирусов. Защита домашних персональных компьютеров и от воздействия вредоносных программ и вирусов. Подсистема защиты корпоративной информации от вредоносных программ и вирусов.

Практическая подготовка: Защита от вредоносных программ. На основании данных варианта задания из Таблицы 1, скачать инсталляционную версию антивирусного пакета. Установить ее на свой ПК, предварительно отключив антивирусный пакет, установленный на нем. Протестировать установленный антивирусный пакет в течение нескольких дней. Изучить

режимы его работы, на основании полученных данных заполнить Таблицу №2 для своего антивирусного пакета по своему варианту. Проверить флешку с его помощью. Сохранить в файле отчета скриншоты основных режимов использования программы-антивируса в формате презентации. Изучить отчеты по анализу рынка антивирусных программ. Определить долю рынка антивирусного ПО, занимаемую программой из своего варианта (столбец №5). Подготовиться к ответам на теоретические вопросы из столбца №6 при защите отчета по работе.

РАЗДЕЛ 2. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1. Основные принципы и методы в области технической защиты информации. ОПК-3.1

Содержание лекции: Направления обеспечения ИБ. Правовая защита Организационная защита. Физические и организационно-технические средства защиты. Технические каналы утечки информации. Способы защиты информации в организации. Общие положения . Защита информации от утечки по визуально оптическим каналам. Общие положения. Средства и способы защиты. Защита информации от утечки по акустическим каналам. Способы и средства защиты. Классификация ЭКМ каналов утечки информации**.** Защита информации от утечки по электромагнитным каналам. Способы и средства защиты. Побочные электромагнитные излучения и наводки (ПЭМИН). Причины возникновения технических каналов утечки информации. Защита информации от утечки по техническим каналам.

Практическая подготовка: Сформулировать требования к защите информации в организации и **р**азработать общие подходы к защите информации от утечек. Сформулировать, посредством каких категорий передается информация. Изобразить в виде схематического рисунка и опишите структуру канала утечки информации. Разработать рекомендации по защите информации от утечек по визуально-оптическому каналу. Разработать рекомендации по защите информации от утечек по акустическому каналу. Разработать рекомендации по защите информации от утечек по электромагнитному каналу. Разработать рекомендации по защите информации от утечек по каналу ПЭМИН.

Тема 2.2. Противодействие несанкционированному доступу к конфиденциальной информации. Социальная инженерия. ОПК-3.1

Содержание лекции: Защита от НСД. Способы доступа посторонних к конфиденциальным сведениям. Для чего предпринимаются попытки доступа к чужой информации. Методы защиты от несанкционированного доступа. Идентификация и аутентификация пользователей. Протоколы секретности для

бумажной документации. Защита данных на ПК. Определение уровней защиты. Предотвращение сетевых атак.

Социальная инженерия: общие вопросы. Как защититься изнутри организации. Социальная инженерия – это приемы, методы и технологии, направленные на получение КИ с помощью психологического воздействия и манипуляций. Типы атак социальной инженерии: фишинг, подложные ссылки, претекстинг, квид про кво, «дорожное яблоко». Дипфейки. Схемы проведения фишинговых атак кибермошенниками. Последствия фишинговых атак для организации. Рекомендации по защите от атак кибермошенников. Два аспекта защитных действий: методологический и практический. Базовые принципы защиты. Обучение пользователей. Профилактические мероприятия (не только обучение, но имитация фишинга). Актуальная документация и инструкция. Ответственные лица в организации. Отдел безопасности или его аналоги. Системы DLP. Три основные функции DLP-систем: блокировка попыток утечек. определение содержимого отправляемых документов, знание потоков отправляемой из организации информации

Практическая подготовка: Сформулируйте главную задачу злоумышленника в процессе фишинговой атаки. Опишите, на каких недостатках человека базируется эта атака. Объясните, какие действия стремятся вынудить вас совершить киберпреступники. Опишите, какие механики они использую при этом. Сформулируйте, что такое социальная инженерия. Сформулируйте типы атак социальной инженерии, дайте характеристику каждому их них. Опишите такие типы атак социальной инженерии, как всевозможные маркетинговые акции, опросы, рассылки; robocall; поддельные номера мобильной связи; мошенничество с угрозами. Опишите схему действия кибермошенников при фишинговой атаке. Сформулируйте, в чем заключается реализация методологического подхода по защите информации в организации. Опишите, в чем заключается практический аспект защиты информации в организации. Опишите функции DLP-систем. Приведите примеры российских DLP-систем. Дайте общие рекомендации по защите информации в организациях в условиях резкого роста фишинговых атак

Тема 2.3. Классификация криптографических методов защиты. Симметричные криптографические алгоритмы

Содержание лекции: Криптография. Термины и определения. Прямая и обратная операциии в криптографии. Понятие криптографичскрго алгоритма. Принцип Керкхоффса**.** Классификация криптографических алгоритмов. Хеширование, хеш-функция. Симметричные алгоритмы шифрования. Шифры замены (подстановки). Шифр Цезаря. Шифр Виженера. Шифры перестановочного типа. Шифр Вернама. Операция XOR. Алгоритм Диффи-Хеллмана. Блочные алгоритмы шифрования. Стандарт шифрования AES. Достоинства и недостатки симметричных систем шифрования.

Практическая подготовка: Изучить теоретический материал и ответить на вопросы: Какой алгоритм описывает шифрование методом Цезаря? В чем преимущество шифров многоалфавитной замены? Что из себя представляет множество алфавитов в шифре Виженера? Какой формулой описывается алгоритм Виженера? Можно ли шифр Цезаря назвать частным случаем шифра Виженера? Что из себя представляет шифр Вернама?
Выполнить шифрование и расшифрование заданного в варианте сообщения методом Цезаря. Создать алгоритм и программу, реализующую этот метод, на одном из языков программирования.

Выполнить шифрование и расшифрование сообщения, заданного в варианте текста сообщения и ключа методом Вижинера. Создать алгоритм и программу, реализующую метод Вижинера на одном из языков программирования. Оформить отчет о выполненной работе в виде презентации

Тема 2.4. Асимметричные криптографические алгоритмы. ОПК-3.1.

Содержание лекции: Асимметричные криптосистемы. Особенность использования открытого и закрытого ключей в асимметричном криптоалгоритме. Использование электронной цифровой подписи. Инфраструктура открытых ключей (PKI, Public Key Infrastructure). Элементы типовой архитектуры PKI. Функции УЦ (Удостоверяющего Центра), как главного компонента инфраструктуры PKI Пример реализации асимметричного алгоритма. Алгоритм RCA. Функция Эйлера. Шифрование и расшифровывание в RSA. Структура криптосистемы PGP. Причины использования алгоритма PGP. Генерация ключа шифрования, шифрование и расшифровка сообщений.

Практическая подготовка: Структура криптосистемы PGP, свободно распространяемая система, одна из лучших. Сгенерировать ключевую пару (из открытого и закрытого ключей). Выбрать тип асимметричного алгоритма: RSA Legacy (v3) - устаревшего формата, который может иметь ограничение по длине ключа (до 2048 бит); RSA v4 -современного формата, совместимого с PGP 7.0 и выше; Diffie-Hellman/DSS (DH/DSS) - алгоритм, использующий шифрование по схеме Эль-Гамаля и подписание по стандарту DSS. Зашифровать данные отправителем, используя открытый ключ получателя. Расшифровать данные получателем на основе применения своего закрытого ключа. Использовать цифровую подпись**.** Цели ее применения в асимметричном алгоритме и технология использования в нем.

Тема 2.5. Цифровая электронная подпись (ЭЦП). Технологии аутентификации. ОПК-3.1.

Содержание лекции: Правовое обоснование использования ЭЦП на основе применения №63-ФЗ «Об электронной подписи». Три вида ЭЦП, функции и особенности получения и применения каждого вида подписи. Аналогия электронного цифрового документа и письма с сургучной печатью. Три элемента цифровой подписи: отпечаток документа, печать и ее цифровой паспорт. Дополнительный файл, который присоединяется к документу на основе их использования. Создание отпечатка документа на основе создания

хэша передаваемого документа. Шифрование хэша, осуществляемое закрытым ключом отправителя, как установка электронной сургучной печати. Присоединение электронного сертификата пользователя завершает формирование ЭЦП. Триединая задача применения цифровой подписи. Реализация алгоритма создания ЭЦП и его составных элементов. Функции усиленной цифровой подписи. Удостоверяющий центр (УЦ) и его функции в процедуре использования ЭЦП. Особенности применения электронной подписи (ЭЦП), начиная с 2024 года.

♦ **Практическая подготовка:** Сформулировать преимущества применения ЭЦП. Описать функции конфиденциальности ЭЦП. Разъяснить почему выполнение этого требования указывает на аутентичность и уникальность автора цифровой подписи. Сформулировать почему ЭЦП не поддается подделке или переносу с документа на документ. Объяснить почему ЭЦП защищает подписанный документ от подделки, а также от изменения или искажения содержащейся в нем информации. Сформулировать почему ЭЦП несет принцип не отречения от подписи, что предотвращает отказ от нее. Объяснить снижение в несколько раз материальных и технических затрат налогоплательщика при использовании ЭЦП. Разъяснить преимущества, предоставляемые налоговой службой при предоставлении отчетности, подписанной ЭЦП. Сформулировать цели использования ЭЦП на стадии цифровизации и электронного документооборота

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.О.02.13 Технологии обеспечения информационной безопасности входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые

можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа – это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы

Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр

Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2. Продумать логику и полноту ответа. 3. Записать ответ, используя четкие компактные формулировки. 4. В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3. Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Оценка по шкале ECTS	**Сумма баллов за все виды учебной деятельности**	**Оценка по государственной шкале**	**Определение**
A	90 – 100	«Отлично»	Отличное выполнение с незначительным количеством неточностей
B	80 – 89	«Хорошо»	в целом правильно выполненная работа с незначительным количеством ошибок (до 10%)
C	75 – 79		в целом правильно выполненная работа с незначительным количеством ошибок (до 15%)
D	70 – 74	«Удовлетворительно»	неплохо, но со значительным количеством недостатков
E	60 – 69		Выполнение удовлетворяет минимальные критерии
FX	35 – 59	«Не удовлетворительно»	с возможностью повторной сдачи
F	0 – 34		с обязательным повторным изучением дисциплины (выставляется комиссией)

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
100 баллов	100 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины Б1.О.02.13 Технологии обеспечения информационной безопасности используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Контрольные вопросы для проведения опроса, задания открытого типа на практических занятиях, контрольные задания

Таблица 5.1.

Распределение баллов по видам учебной деятельности (БРС)

Раздел/Темы	Формы текущего контроля		КТ
	УО	ПЗ	
Р-1. / Т-1.1	3	3	6
Р-1. / Т-1.2	3	5	
Р-1. / Т-1.3	3	3	7
Р-1. / Т-1.4	3	5	
Р-2. / Т-2.1	3	4	8
Р-2. / Т-2.2	3	5	
Р-2. / Т-2.3	4	4	12
Р-2. / Т-2.4.	3	4	
Р-2. / Т-2.5.	4	5	
Итого: 100 б	**29**	**38**	**33**

УО – устный опрос;
ТЗ – тестовое задание;
КЗ – контрольные задания;
ПЗ – практическое занятие;
Д – доклад;
КТ – контрольные точки.

Критерии оценивания опроса:

Балы	Описание критерия
4	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
2-3	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
1	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал

0* - в журнал академической группы не выставляется

Критерии оценивания практических занятий:

Балы	Описание критерия	
4-5	Свыше 90% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
2-3	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
1	Реализовано более 50% поставленных задач	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0	Реализовано менее 30% поставленных задач.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

0* - в журнал академической группы не выставляется

Критерии оценивания контрольных заданий:

Балы	Описание критерия
10-12	Обучающимся задание выполнено без ошибок и в полном объеме.
7-9	Обучающимся в целом задание выполнено, имеются отдельные неточности или недостаточно полные ответы, не содержащие ошибок.
5-6	Обучающимся допущены отдельные ошибки при выполнении задания
0-4	У обучающегося отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

0* - в журнал академической группы не выставляется

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

РАЗДЕЛ 1. ТЕХНОЛОГИИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИБ

Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба

1. Контрольные вопросы для проведения опроса:
2. Сформулируйте, чем отличаются информационные ресурсы от материальных
3. Объясните, почему важно не блокировать информационные ресурсы и сервисы, а научиться распознавать угрозы, купировать их различными методами и квалифицированно решать задачи в сети
4. Разъясните, что такое компьютерное преступление. Классифицируйте компьютерные преступления.

Практические занятия:

Задания открытого типа с развернутым ответом.

Установить программный продукт хранения паролей KeePass, скачав его с интернет-ресурса https://keepass.info/

Создать свою базу паролей для почты, работы в корпоративной сети, социальной сети и других аккаунтах. Обосновать преимущества использования данного приложения

Сгенерировать с ее помощью пароль уровня Strong. Использовать его для создания копии своей базы паролей, сохранив ее на локальном носителе.

Скачать базу паролей «Portable» и установить ее для постоянной работы со сменного носителя.

Разъяснить выигрышные стороны базы паролей портативной базы KeePass

Тема 1.2. Угрозы информационной безопасности. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Контрольные вопросы для проведения опроса:

1. Объясните, что такое угроза информационной безопасности ИС
2. Разъясните, что такое источник угрозы безопасности информации
3. Опишите угрозу «Посредничество в обмене незашифрованными ключами (атака man-in-the-middle)» и способы защиты от нее.
4. Опишите угрозу «DDoS (distributed DoS)» и способы защиты от нее.

Практические занятия:

Задания открытого типа с развернутым ответом.

Скачать программу генерации паролей Advanced Password Generator по ссылке
https://drive.google.com/open?id=1Q7qLTrCefuZNJ3XDzq0FFZ2lWIsINW-S

Сгенерировать при помощи скачанной программы группы паролей по следующей схеме: 8-9(10)-12-20 символов в пароле (буквы / буквы+цифры / буквы+цифры+спецсимволы).

При помощи интернет ресурсов https://bitwarden.com/password-strength/, https://2ip.ru/passcheck/ и https://password.kaspersky.com/ru/ проверьте сгенерированные пароли.

Сохранить в таблице с двумя столбцами пароль (в левом столбце) результат проверки его криптостойкости в правом столбце

Сформулировать и описать процесс изменения стойкости паролей в зависимости от их структуры и количества символов в нем (описания подтвердить скриншотами).

Для каждого пароля дать ответ на вопрос «Являются ли он надежным?»

Сформулировать требования по созданию надежных паролей и изложить их

Тема 1.3. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Контрольные вопросы для проведения опроса:

1. Сформулируйте, из каких структурно-функциональных элементов состоят ИС и каким угрозам они могут быть подвержены
2. Разъясните, что такое естественные угрозы (случайные) ИС
3. Сформулируйте, что такое искусственные угрозы ИС
4. Перечислите непреднамеренные искусственные угрозы ИС
5. Перечислите виды нарушений работоспособности систем и несанкционированного доступа к информации.

Практические занятия:

Задания открытого типа с развернутым ответом.

Необходимо создать диск и зашифровать его с помощью BitLocker:

Создать новый файл виртуального диска (VHD) на своем ПК.

Выберите элемент управления дисками.

Открыть меню «Действие» в окне «Управление дисками» и выбрать «Создать виртуальный жесткий диск (VHD)

Создать и прикрепить новый файл виртуального диска (VHD)

Инициализировать новый виртуальный диск

Создать раздел на виртуальном диске. Нажать на нераспределенное пространство правой кнопкой мыши и выберите «Создать простой том». Например, том Z1

Запустить Мастер создания простого тома. Указать его размер (100 М).

На третьем шаге указать символ логического устройства для него (например, Y)

На четвертом шаге задать форматирование его в системе NFTS (быстрое форматирование)

Мастер завершит свою работу и выдаст диалоговое окно. В нем нажать «Готово».

Шифровать новый виртуальный диск с помощью BitLocker. Нажать диск в Проводнике с помощью правой кнопки мыши и выбрать «Пароль при шифровании диска Z с помощью BitLocker»

Например, VHDYy123 (8 символов)

Сохранить в файл (пароль будет сохранен как файл в указанной папке).

Начать процесс шифрования

По его завершению

Скопировать все данные Темы 1 в новый виртуальный диск, зашифрованный BitLocker.

Чтобы отключить диск, щелкнуть диск с помощью правой кнопки мыши в Проводнике и выбрать «Извлечь»

После этого диск с замочком исчезает из представления в Проводнике, но на диске G: остаются диски VHD и VHD1. При двойном щелчке по диску VHD1 появится сообщение о том, что он заблокирован программой шифрования дисков BitLocker, а в правом верхнем углу экрана появится окошко для ввода пароля для его разблокировки.

Тема 1.4. Технологии защиты от вредоносных программ и спама. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность

Контрольные вопросы для проведения опроса:

1. Опишите этапы жизненного цикла вредоносных программ.
2. Опишите основные этапы развития современных вредоносных программ.
3. Сформулируйте, каковы основные тенденции развития антивирусного программного обеспечения.
4. Разъясните, какие особенности развития информационных технологий способствуют распространению вредоносных программ и угроз с их стороны на уровне обеспечения информационной безопасности организации
5. Объясните, какие особенности развития информационных технологий способствуют распространению вредоносных программ и угроз с их стороны на уровне обеспечения информационной безопасности государства? Приведите примеры.
6. Объясните, чем троян отличается от червя и в чем они схожи

Практические занятия:

Задания открытого типа с развернутым ответом.

Скачать и установить скачать инсталляционную версию антивирусного пакета 360Total Sequrity (https://www.360totalsecurity.com/ru).

Установить ее на свой ПК, предварительно отключив антивирусный пакет, установленный на нем.

Протестировать установленный антивирусный пакет в режиме «Быстрой проверки» для своего ПК

Далее осуществить в режиме «Выборочной проверки» тестирование собственного флеш-устройства

Изучить режимы его работы программы, привести его характеристику на наличие режимов работы, приведенных в таблице 1.

Скачать и установить инсталляционную версию антивирусного пакета Kaspersky Free (https://www.kaspersky.ru/downloads/free-antivirus?ysclid=m0iizlg0i4963699299) на свой ПК

Протестировать установленный антивирусный пакет в режиме «Быстрой проверки».

Далее осуществить в режиме «Выборочной проверки» тестирование собственного флеш-устройства

Изучить режимы его работы программы, привести его характеристику на наличие следующих режимов работы:

Таблица 1

№	Режим использования	Название пакета	Достоинства	Недостатки
1.	Защита от руткитов и шпионских программ			
2.	Технология DeepScreen			
3.	Режимы Hardened («белый» список приложений)			
4.	Веб-защита			
5.	Очистка браузеров «Browser Cleanup»			
6.	Проверка обновлений приложений («Software Updater»)			
7.	Безопасность домашней сети (Home Network Security)			
8.	Сканирование HTTPS			
9.	Безопасное удаление документов			

РАЗДЕЛ 2. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1. Основные принципы и методы в области технической защиты информации

Контрольные вопросы для проведения опроса:

1. Сформулируйте, что такое криптография и в чем заключается главная задача криптографии
2. Сформулируйте, кто является «противником» в криптографии Составьте модель противника в криптографии.
3. Опишите, что такое шифр и ключ в криптографии
4. Сформулируйте, что такое криптографическиий алгоритм (КА).

5. Опишите, в чем заключается Принцип Керкхоффса? Как он применяется на практике

Практические занятия:

Задания открытого типа с развернутым ответом.

Привести классификацию криптографических алгоритмов (КА).

Привести примеры бесключевые КА, одноключевые КА и двухключевые КА

Сформулировать ответ на вопрос: «На какие алгоритмы разделяются блочные алгоритмы?».

Описать характеристики блочного шифрования

Сформулировать характеристики поточного шифрования

Дать определение хеш-фуекции

Перечислить все характеристики хеш-функции

Привести пример онлайн-хеширования текста

Продемонстрировать пример нарушения целостности передаваемой информации, на основе применения предлагаемого онлайн-хеширования

Тема 2.2. Противодействие несанкционированному доступу к конфиденциальной информации. Социальная инженерия

Контрольные вопросы для проведения опроса:

1. Разъясните, что такое социальная инженерия
2. Объясните, что в условиях информационного общества облегчает кибермошенникам задачу получения доступа к конфедициальным данных граждан РФ
3. Сформулируйте, что такое фишинг
4. Разъясните, в чем заключается вид мошенничества использование подложных ссылок
5. Разъясните, что означает технология дип фейков? В чем проявляется ее растущая опасность?
6. Опишите, возможные последствия совершенной кибератаки для вашей организации?

Практические занятия:

Задания открытого типа с развернутым ответом.

Дать опреление системе DLP

Перечислить основные функции системы DLP

Изучить современную российскую DLP-систему компании InfoWatch Traffic Monitor (https://www.infowatch.ru/zaschita-dannykh-ot-utechek/dlp-sistema-traffic-monitor)

Описать как в InfoWatch Traffic Monitor осуществляется Контроль информационных потоков и предотвращение неправомерных действий с информацией

Описать как в InfoWatch Traffic Monitor осуществляется мониторинга действий сотрудников (персонала

Описать как в InfoWatch Traffic Monitor визуализируется данные DLP-системы Traffic Monitor в виде статистики и графа связей

Разъяснить за счет чего в DLP-системе Traffic Monitor происходит быстрое и эффективное расследование инцидентов

Описать как в InfoWatch Traffic Monitor осуществляется идентификация и прогнозирование рисков

Тема 2.3. Классификация криптографических методов защиты. Симметричные криптографические алгоритмы

Контрольные вопросы для проведения опроса:

1. Сформулируйте, какой алгоритм описывает шифрование методом Цезаря
2. Сформулируйте, что из себя представляет множество алфавитов в криптоалгоритме Виженера
3. Сформулируйте, можно ли шифр Цезаря назвать частным случаем шифра Виженера
4. Сформулируйте, в чем заключается основная особенность алгоритма хеширования
5. Опишите особенности симметричных алгоритмов шифрования.
6. Опишите алгоритм Диффи-Хеллмана. Какую роль он сыграл в развитии криптографии симметричных алгоритмов шифрования?

Практические занятия:

Задания открытого типа с развернутым ответом.

Описать алгоритм шифрования методом Цезаря

Задать значение небольшого тектового сообщения

Задать значение ключа для шифрования методом Цезаря

Зашифровать сообщение методом Цезаря, составив программу на

одном из языков программтрования

Продемонстировать выполнение прямой операции с помощью составленной программы

Расшифровать полученное сообщение с помощью этой же программы Продемонстировать выполнение обратной операции с помощью составленной программы

Описать алгоритм шифрования методом Вижинера

Задать значение небольшого тектового сообщения

Задать значение ключа для шифрования методом Вижинера

Зашифровать сообщение методом Вижинера, составив программу на одном из языков программтрования

Продемонстировать выполнение прямой операции с помощью составленной программы

Расшифровать полученное сообщение с помощью этой же программы Продемонстировать выполнение обратной операции с помощью составленной программы

Тема 2.4. Асимметричные криптографические алгоритмы.

Контрольные вопросы для проведения опроса:

1. Сформулируйте отличительные особенности асимметричных криптосистем.
2. Опишите преимущества и недостатки асимметричных криптосистем
3. Разъясните, какую роль в инфраструктуре открытых ключей (Public Key Infrastructure, PKI) играет удостоверяющий Центр (УЦ)
4. Опишите функции сертификатов УЦ, а также их содержание
5. Опишите алгоритм RCA. Разъясните, какую роль в его реализации выполняет функция Эйлера
6. Сформулируйте преимущества асимметричных криптосистем

Практические занятия:

Задания открытого типа с развернутым ответом.

Пользуясь асимметричным алгоритмом RCA, передать слово «Эйлер»

Выполнить прямое преобразование (шифрование)

Затем выполнить обратное преобразование (расшифрование)

Для выполнения задания использовать следующий алфавит:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

Тема 2.5. Цифровая электронная подпись (ЭЦП). Технологии аутентификации

Контрольные вопросы для проведения опроса:

1. Сформулируйте, какие функции выполняет электронная цифровая подпись (ЭЦП).
2. Опишите преимущества применения электронной цифровой подписи
3. Опишите правовую основу применения ЭЦП в РФ. Когда в Закон о ЭЦП были внесены последние на данный момент изменения?
4. Сформулируйте, в чем заключается принципиальное отличие ЭЦП от обычной рукописной подписи
5. Опишите реализацию алгоритма заверения документа личной подписью в доинформационную эпоху. Какие элементы участвуют в этом процессе?
6. Опишите реализацию алгоритма создания ЭЦП и его составных элементов в информационную эпоху

Практические занятия:

Задания открытого типа с развернутым ответом.

Дать определение понятию «электронная цифровая подпись (ЭЦП)»

Разъяснить почему ЭЦП обеспечивает контроль целостности передаваемого документа

Доказательно объяснить вследствие чего ЭЦП обеспечивает защиту от изменений (подделки) передаваемого или подписываемого текста

Сформулировать, по какой причине ЭЦП обеспечивает для лица, подписавшего документ, невозможность отказа от авторства подписи

Объяснить, почему в подписываемых объемных документах, ЭЦП часто ставится не сам документ, а на его хэш

Перечислить преимущества, которые предоставляет хэш

5.3. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ-1

Задание 1. Установить последовательность операций в работе с информацией в определении Н.Винера

ПРЕАМБУЛА

Решение стандартных задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ИКТ и с учетом основных требований информационной безопасности, основано на ключевой категории, которой является определение информации, сформулированное Н.Винером. В этом определении, основанном на нескольких определениях, важна последовательность операций по работе с информацией. Установите правильную последовательность этих операций

Прочитайте текст и установите последовательность.

Информация — сведения об окружающем мире (объектах, явлениях, событиях, процессах и т.д.), которые уменьшают имеющуюся степень неопределенности, неполноты знаний, отчужденные от их создателя и ставшие сообщениями (выраженными на определенном языке в виде знаков, в том числе и записанными на материальном носителе), которые можно воспроизводить путем передачи людьми устным, письменным или другими способами (с помощью условных сигналов, технических и вычислительных средств и т.д.).

В этом определении, построенном на ряде других определений, для нас важно следующее:

1. Информация — это не любые сведения, она несет в себе нечто новое, уменьшающее имеющуюся неопределенность;
2. она существует вне ее создателя, это отчужденное от ее создателя знание; знание — отражение действительности в мышлении человека;
3. сообщение может быть записано на материальном носителе (т.е. является формой передачи информации);
4. оно доступно для воспроизведения без участия автора;
5. информация стала сообщением, так как она выражена на определенном языке в виде знаков.

Запишите соответствующую последовательность цифр слева направо:

Задание 2. Что такое компьютерное преступление

БК (комбинированный), задание на выбор одного ответа и установление последовательности

Текст задания

ПРЕАМБУЛА

Сегодня компьютерная преступность растет по нескольким причинам:

- широкое распространение компьютерных технологий и средств связи. компьютерные системы, интернет, социальные сети стали неотъемлемой частью жизни большинства людей, что привело к увеличению количества преступлений, совершаемых с использованием информационных технологий;
- информационно-техническое переоборудование предприятий, учреждений и организаций. Наполнение их новой компьютерной техникой, программным обеспечением, базами данных создало благоприятные условия для противоправных деяний;
- возможность получения экономической выгоды. Противоправные деяния с использованием компьютерной информации могут быть связаны с получением значительных денежных средств или других выгод;
- глобализация информационных процессов. Появлению глобальных информационных сетей и их использованию в целях совершения преступлений способствует то, что киберпреступникам проще объединять усилия и совершать всё более сложные деяния.

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор.

Что такое компьютерные преступления? Выберите правильный вариант ответа и обоснуйте его.

А. Компьютерные преступления - это исключительно взлом компьютеров правительственных организаций.

Б. К разряду компьютерных преступлений следует отнести те из них, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер.

В. Компьютерные преступления — это установка нелицензионного программного обеспечения на рабочий компьютер.

Г. Компьютерные преступления — это любые действия, совершаемые с помощью компьютера, включая игру в видеоигры и общение в социальных сетях.

Д. Компьютерные преступления — это покупка нового оборудования для своего компьютера.

Задание 3. Что такое информационный объект

БК (комбинированный), задание на выбор одного ответа и установление последовательности

Текст задания

Сегодня мир переживает новый виток технологического развития –

революцию в сфере информации. Формируется новое информационное пространство, которое оказывает мощное воздействие на все сферы жизни общества. Под информационным пространством здесь понимается совокупность объектов, вступающих друг с другом в информационное взаимодействие, а также технологии этого взаимодействия – Интернет как глобальное информационное пространство.

В условиях информационного общества информация становится важнейшей областью исторического соперничества на мировой арене, она приобретает форму активной борьбы, называемой информационной войной (борьбой). Ожесточенная борьба в области информации – борьба за контроль над наиболее ценным из всех известных ресурсов – информацией – разворачивается со все нарастающей силой. Этому способствует множество факторов, влияющих на структуру и содержание информационного пространства. Выделим две группы факторов: технологическую и социально-политическую. Сформулируйте, как вы понимаете эти две группы факторов в информационной войне, постоянно ведущейся против нашей страны

Прочитайте текст, выберите один правильный ответ и запишите аргументы, обосновывающие выбор.

Что такое информационный объект? Выберите правильный вариант ответа и обоснуйте его.

А. Информационный объект - это исключительно запоминающее устройство для хранения информации, например, жёсткий диск или флешка.

Б. Информационный объект - это только текстовый объект, созданный пользователем.

В. Информационный объект – среда, в которой информация создается, передается, обрабатывается или хранится.

Г. Информационный объект - это программа, управляющая компьютером, не содержащая данных.

Д. Информационный объект - это любой объект, который можно найти в глобальной сети.

КТ-2

Задание 1. Две группы угроз информационной безопасности

ПК- повышенный комбинированный тип, задание с выбором двух ответов и обоснованием выбора

Текст задания

Решение стандартные задачи профессиональной деятельности на основе применения ИКТ и с учетом основных требований информационной безопасности, невозможно без обеспечения информационной безопасности субъектов информационных отношений. Одной из ключевых категорий

информационной безопасности является понятие информационных угроз

Угроза информационной безопасности ИС – это возможность реализации воздействия на информацию, обрабатываемую в ИС, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты ИС, приводящего к их утрате, уничтожению или сбою функционирования.

Непосредственная реализация угрозы называется атакой на ИБ. Атака использует уязвимости и нарушает информационную безопасность объектов. Именно поэтому угрозы необходимо изучать, классифицировать и определять меры, обеспечивающие защиту от каждой из них.

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

Угрозы информационной безопасности разбиваются на две большие группы. Какие это группы?

А. Визуальные угрозы.
Б. Естественные (случайные) угрозы.
В. Искусственные угрозы.
Г. Электромагнитные угрозы.
Д. Звуковые угрозы.

Запишите выбранный ответ и аргументы, обосновывающие выбор ответа него:

Задание 2. Влияние технологических и геополитических факторов на развитие информационных войн

ПО. Повышенный открытый, задание с двумя развернутыми ответами
Понимание принципов работы современных информационных технологий и программных средств, невозможно без обеспечения информационной безопасности субъектов

Текст задания
Прочитайте текст и запишите два развернутых обоснованных ответа

Сегодня мир переживает новый виток технологического развития – революцию в сфере информации. Формируется новое информационное пространство, которое оказывает мощное воздействие на все сферы жизни общества. Под информационным пространством здесь понимается совокупность объектов, вступающих друг с другом в информационное взаимодействие, а также технологии этого взаимодействия – Интернет как глобальное информационное пространство.

В условиях информационного общества информация становится важнейшей областью исторического соперничества на мировой арене, она

приобретает форму активной борьбы, называемой *информационной войной (борьбой),* которая постоянно ведется против Российской Федерации. Ожесточенная борьба в области информации – борьба за контроль над наиболее ценным из всех известных ресурсов – информацией – разворачивается со все нарастающей силой. Этому способствует множество факторов, влияющих на структуру и содержание информационного пространства. Выделяется две группы факторов: технологическая и социально-политическая.

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

Объясните ваше понимание двух групп факторов, влияющих на ведение информационной войны.

1) Объясните, что такое технологические факторы, влияющих на развитие информационной войны.

2) Разъясните, что такое социально-политические факторы, влияющих на развитие информационной войны.

Задание 3. Определение информационной безопасности

ПО

ПО. Повышенный открытый, задание с двумя развернутыми ответами

Понимание принципов работы современных информационных технологий и программных средств, невозможно без обеспечения информационной безопасности субъектов

Текст задания

Прочитайте текст и запишите два развернутых обоснованных ответа

Сегодня мир переживает новый виток технологического развития – революцию в сфере информации. Формируется новое информационное пространство, которое оказывает мощное воздействие на все сферы жизни общества. Под информационным пространством здесь понимается совокупность объектов, вступающих друг с другом в информационное взаимодействие, а также технологии этого взаимодействия – Интернет как глобальное информационное пространство.

В условиях информационного общества информационная безопасность становится ключевым понятием. Понятие информационной безопасности не менее многогранно, чем понятие самой информации, и зависит от контекста, в котором применяется.

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор.

1) Объясните, что такое информационная безопасность в широком смысле.

2) Разъясните, что такое безопасность информации, то есть ИБ в более узком смысле.

5.4. Типовые оценочные материалы промежуточной аттестации.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме *зачета* в пятом семестре.

6.2. Типовые оценочные материалы промежуточной аттестации.

Вопросы для зачета:

РАЗДЕЛ 1. ТЕХНОЛОГИИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИБ

Тема 1.1 Основные понятия ИБ. ИБ в системе национальной безопасности России. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба

1. Охарактеризовать информационную войну как угрозу информационной безопасности национального уровня на основе Доктрины информационной безопасности РФ
2. Объекты и субъекты информационного пространства. Привести примеры.
3. Субъекты информационных отношений и их интересы.

Тема 1.2. Угрозы информационной безопасности. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

4. Три уровня управления политикой безопасности на предприятии.
5. Варианты построения виртуальных защищенных каналов.
6. Понятие «модели злоумышленника». Привести примеры.
7. Конфиденциальность информации. Способы обеспечения конфиденциальности информации в организации.

Тема 1.3. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

8. Практические методы аутентификации, используемые в настоящее время

9. Классификация каналов проникновения в систему и утечки информации
10. Политика информационной безопасности организации.
11. Содержание политики безопасности организации.
12. Определение информационной безопасности и ее составляющие.

Тема 1.4 Технологии защиты от вредоносных программ и спама. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность

13. Причины роста компьютерной преступности. Компьютерные преступления против государственных и общественных интересов.
14. Ключевые категории (понятия) безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.
15. Классификация вредоносных программ.
16. Сигнатурные методы обнаружения вредоносного ПО.
17. Проактивные методы обнаружения вредоносного ПО.
18. Тенденции развития современных антивирусных программ
19. Модули и режимы работы современных антивирусных программ.
20. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
21. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
22. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.

РАЗДЕЛ 2. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

23. Тема 2.1. Основные принципы и методы в области технической защиты информации
24. Методика создания демилитаризованных зон в корпоративной сети предприятия
25. Защита информации от утечки по электромагнитным каналам
26. Технические каналы утечки информации. Защита от утечек информации по техническим каналам
27. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
28. Технология обеспечения безопасности ИС при беспроводном соединении
29. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.

Тема 2.2. Противодействие несанкционированному доступу к конфиденциальной информации. Социальная инженерия

30. Система обнаружения и предотвращения вторжений.
31. Технологии обеспечения безопасности в ОС Windows 7.
32. Способы защиты информации в организации. Характеристика защитных действий
33. Защита информации от утечки по визуально оптическим каналам.
34. Способы защиты информации в организации. Характеристика защитных действий
35. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
36. Технология обеспечения безопасности ИС при беспроводном соединении

Тема 2.3. Классификация криптографических методов защиты. Симметричные криптографические алгоритмы

37. Термины и определения криптографии.
38. Классификация криптографических алгоритмов
39. Симметричные алгоритмы шифрования. Примеры
40. Криптографический алгоритм Цезаря. Преимущества и недостатки.
41. Криптографический алгоритм Виженера. Преимущества и недостатки.
42. Технологии биометрической аутентификации пользователя.
43. Преимущества и недостатки симметричных алгоритмов шифрования
44. Проблемы безопасности IP-сетей
45. Порядок использования систем с симметричными ключами.

Тема 2.4. Асимметричные криптографические алгоритмы

46. Преимущества и недостатки асимметричных систем шифрования.
47. Порядок использования систем с асимметричными ключами
48. Охарактеризовать методы социальной инженерии и технологию борьбы с ними

Тема 2.5. Цифровая электронная подпись (ЭЦП). Технологии аутентификации

49. Технологии строгой аутентификации пользователя.
50. Технология использование электронной цифровой подписи.
51. Классификация механизмов аутентификации пользователей

6.3. Критерии и шкала оценивания на основе БРС.

Соответствие государственной шкалы оценивания академической успеваемости и шкалы ECTS при дифференцированном зачете

Оценка по шкале ECTS	**Сумма баллов за все виды учебной деятельности**	**Оценка по государственной шкале**	**Определение**
A	90 – 100	«Отлично»	Отличное выполнение с незначительным количеством неточностей
B	80 – 89	«Хорошо»	в целом правильно выполненная работа с незначительным количеством ошибок (до 10%)
C	75 – 79		в целом правильно выполненная работа с незначительным количеством ошибок (до 15%)
D	70 – 74	«Удовлетворительно»	неплохо, но со значительным количеством недостатков
E	60 – 69		выполнение удовлетворяет минимальные критерии
FX	35 – 59	«Не удовлетворительно»	с возможностью повторной сдачи
F	0 – 34		с обязательным повторным изучением дисциплины (выставляется комиссией)

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий

Компьютер с операционной системой Windows, на котором установлена одной последних версий браузера Chrome или ЯндексБраузер.

7. Методические материалы по освоению дисциплины

Получение углубленных знаний по изучаемой дисциплине достигается за счет дополнительных часов к аудиторной работе самостоятельной работы студентов. Выделяемые часы целесообразно использовать для знакомства с дополнительной научной литературой по проблематике дисциплины, анализа научных концепций и современных подходов к осмыслению рассматриваемых проблем. К самостоятельному виду работы студентов относится работа в библиотеках, в электронных поисковых системах и т.п. по сбору материалов, необходимых для проведения практических занятий или выполнения конкретных заданий преподавателя по изучаемым темам. Студенты могут установить диалог с преподавателем, получать консультации по выполнению заданий. В качестве оценочных средств на протяжении семестра используются тестовые и иные задания.

Обучение по дисциплине «Технологии обеспечения информационной безопасности» предполагает изучение курса на аудиторных занятиях (лекции, практические занятия) и самостоятельную работу студентов. Практические занятия дисциплины предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения студент 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.

Работа обучающегося на лекции:

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся.

Подготовка к практическим занятиям:

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенных методических указаний. Выполняемые практические задания становятся основой для выполнения курсового проекта по дисциплине Б1.В.01.06 «Технологии обеспечения информационной безопасности».

Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Устный опрос.

2. Обсуждение теоретических вопросов, определенных программой дисциплины.

3. Выполнение практических заданий с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома.

4. Подведение итогов занятия.

Работа с литературными источниками:

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою

индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1 Основная литература

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.

2. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : МИСИС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/360344 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.

3. Михнев, И. П. Информационная безопасность : учебное пособие / И. П. Михнев. — Москва : Дело РАНХиГС, 2019. — 82 с. — ISBN 978-5-7786-0776-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/466877 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 7-е изд., стер. — Санкт-Петербург : Лань, 2026. — 124 с. — ISBN 978-5-507-56325-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/515187 (дата обращения: 06.06.2026). — Режим доступа: для авториз. пользователей.

8.2 Дополнительная литература

1. Беккалиева, Наталья Климентьевна. Информационная безопасность : практикум для студентов вузов / Н. К. Беккалиева ; Федеральное государственное бюджетное образовательное учреждение высшего образования Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Поволжский институт управления им. П. А. Столыпина. — Саратов : Поволжский ин-т упр. им. П. А. Столыпина - фил. РАНХиГС, 2019. — 97 с. : табл. : 21 см.; ISBN 978-5-8180-0573-7.

8.3 Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации. – Текст : электронный // Сайт Президента Российской Федерации. – URL: http://www.kremlin.ru/acts/constitution

8.4 Интернет-ресурсы

1. Информационно-правовой портал ГАРАНТ.РУ. – URL: https://www.garant.ru/
2. Научная электронная библиотека eLIBRARY.RU. – URL: https://elibrary.ru/
3. Научная электронная библиотека «КиберЛенинка». – URL: https://cyberleninka.ru
4. Электронно-библиотечная система «Лань». – URL: http://e.lanbook.com
5. Федеральный закон от 27 июля 2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/
6. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных». URL: https://www.consultant.ru/document/cons_doc_LAW_112701/
7. Федеральный закон от 26.07.2017 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_220885/
8. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_48699/
9. Федеральный закон от 6 апреля 2011 г.63-ФЗ «Об электронной подписи». URL: https://www.consultant.ru/document/cons_doc_LAW_112701/

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

Материально-техническое обеспечение дисциплины включает в себя:

- лекционные аудитории, оборудованные видеопроекционнымоборудованием для презентаций, средствами звуковоспроизведения, экраном;
- помещения для проведения семинарских и практических занятий, оборудованные учебной мебелью.

Дисциплина поддержана соответствующими программными продуктами с открытой лицензией: KeePass, VeraCrypt, 360 Total Sequrity.

Вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Помещения для самостоятельной работы обучающихся включают следующую оснащенность: столы аудиторные, стулья, доски аудиторные, компьютеры с подключением к локальной сети института (для компьютерных аудиторий) и Интернет. Для изучения учебной дисциплины используются автоматизированная библиотечная информационная система и электронные библиотечные системы.