МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Экономический факультет
Кафедра социально-экономической статистики и демографии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОЙ ОРГАНИЗАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

38.03.02 Менеджмент
Код и наименование направления подготовки/специальности

Менеджмент и цифровая трансформация бизнес-процессов компании
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *Очно-заочная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2025

Информационная безопасность цифровой организации
Рабочая программа дисциплины
Составитель:
Канд.техн.наук, доц. Сысоева Л.А.

УТВЕРЖДЕНО:

Протокол заседания кафедры
№4 от 22.11.2024 года

ОГЛАВЛЕНИЕ

1 Пояснительная записка

1.1 Цель и задачи дисциплины

Цель дисциплины – формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в информационных и вычислительных системах.

Задачи дисциплины:

1. Развить навыки по описанию информационной безопасности и реализации бизнес-процессов предприятия.
2. Сформировать у обучающихся компетенции в области безопасности современных цифровых программных продуктов в сфере управления деятельностью предприятия.
3. Развить навыки применения системного подхода к безопасности, информатизации и автоматизации решения прикладных задач.
4. Развить навыки формирования обобщенных требований к информационной системе предприятия, её структуре и основным данным.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-4 Способность выявлять, собирать и анализировать информацию для формирования возможных решений, описывать возможные решения	ПК-4.1 Выявляет, собирает и анализирует информацию для формирования возможных решений ПК-4.2 Описывает возможные решения	**Знать** - нормативно-правовые основы информационной безопасности в Российской Федерации; - требования безопасности к информационным системам; - способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности. **Уметь** - разрабатывать политику информационной безопасности программных продуктов и организаций на основе нормативно-правовых документов; - проводить анализ предметной области и выявлять информационные угрозы в организации. **Владеть** - навыками документирования инцидентов и процессов информационной безопасности; - навыками управления инцидентами информационной безопасности.

1.2 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность цифровой организации» входит в часть дисциплин, формируемой участниками образовательных отношений, ОПОП образовательной программы бакалавриата по направлению подготовки 38.03.02 Менеджмент, направление «Менеджмент и цифровая трансформация бизнес-процессов компании».

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Базы данных», «Управление человеческими ресурсами и HR-аналитика», «Современные технологии разработки программного обеспечения», «Цифровые платформы управления бизнес-процессами».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Теория и практика процессного управления», «Облачные технологии», «Центры обработки данных», «Риск-менеджмент», «Бизнес-архитектура организации».

2 Структура дисциплины

Структура дисциплины для очной формы обучения
Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., в том числе контактная работа обучающихся с преподавателем 24 ч., самостоятельная работа обучающихся 84 ч.
Форма контроля – экзамен.

Семестр	Тип учебных занятий	Количество часов
7	Лекция	8
7	Семинар	16
	Всего:	24

3 Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Методологические основы организации системы защиты информации	Подходы к проектированию системы защиты информации (СЗИ). Понятие системы защиты информации. Назначение, принципы построения системы защиты информации. Стратегия защиты информации. Выработка политики безопасности. Основные требования, предъявляемые СЗИ. Методология защиты информации. Основные положения теории систем. Основы методологии принятия управленческого решения.
2	Определение состава защищаемой информации	Методика определения состава защищаемой информации. Классификация информации по видам тайн и степеням конфиденциальности. Определение объектов защиты.
3	Каналы и методы несанкционированного доступа к информации	Источники дестабилизирующего воздействия на информацию. Методика выявления способов воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию. Выявление каналов доступа к информации. Соотношение между каналами и источниками воздействия на информацию. Модель потенциального нарушителя.

4	Технология построения СЗИ	Понятие модели объекта. Значение моделирования процессов защиты информации. Архитектурное построение СЗИ. Технологическое построение СЗИ. Этапы разработки СЗИ. Факторы, влияющие на выбор состава СЗИ. Модель системы автоматизированного проектирования защиты информации. Задача организационного обеспечения защиты информации. Анализ и оценка угроз информационной безопасности объекта. Классификация методов и средств инженерно-технической защиты информации и объектов информатизации. Методы защиты информации специальными средствами.
5	Программно-аппаратное обеспечение информационной безопасности	Вредоносные программы и антивирусные программы. Идентификация и аутентификация. Методы разграничения доступа. Регистрация и аудит событий информационных систем. Межсетевое экранирование. Технология виртуальных частных сетей. Современные технологии криптографии. Симметричные системы шифрования. Ассиметричные системы шифрования. Электронно-цифровая подпись. Управление криптографическими ключами.
6	Нормативно-правовое обеспечение системы защиты информации	Значение нормативно-правового обеспечения. Состав нормативно-правового обеспечения. Порядок разработки и внедрения документов.
7	Управление системой защиты информации	Понятие и цели управления СЗИ. Планирование деятельности управления СЗИ. Архитектура систем управления информационной безопасностью. Методика управления инцидентами. Структура и задачи группы реагирования на инциденты, ее состав и процесс создания. Оценка эффективности реагирования на инциденты. Методы обнаружения инцидентов. Анализ аномалий информационной безопасности. Кадровое обеспечение СЗИ. Подбор персонала. Подготовка персонала для работы в новых условиях. Мотивация. Разработка кодекса корпоративного поведения.

4 Образовательные технологии

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5 Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - защита отчета по практической работе	12 баллов	60 баллов

Промежуточная аттестация: зачет с оценкой		40 баллов
Итого за семестр		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 оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	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, 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»/ «зачтено (хорошо)»/ «зачтено»	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.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	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	«неудовлетворите льно»/ не зачтено	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.

Критерии оценивания практических работ:

Критерии оценивания / Уровень требований к обучающемуся	Макс. кол-во баллов
Текущий контроль, всего в т.ч.:	**60**
Практическая работа	**12**

Задания выполнены не полностью и (или) допущены две и более ошибки или три и более недочета	1-6
Задания выполнены полностью, но допущены два-три недочета, в т. ч. при ответе на контрольные вопросы	7-9
Задания выполнены полностью, возможна одна неточность, ответы на контрольные вопросы правильные	10-12

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

Примеры тестов

Основные свойства защищенной информации:
а) конфиденциальность, скрытность, доступность
б) целостность, конфиденциальность, доступность
в) актуальность, целостность, конфиденциальность
г) полезность, актуальность, целостность

Что не является противоправным действием в области информационной безопасности:
а) хищение информации;
б) копирование компьютерной информации;
в) уничтожение информации;
г) шифрование информации;
д) повреждение информации

К какому виду защиты информации относится установка антивирусных программ?
а) техническая;
б) физическая;
в) криптографическая;
г) правовая ;
д) программная

Какой орган государственной власти осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных?
а) ФСТЭК России;
б) ФСБ России;
в) СВР России;
г) МВД России;
д) Роскомнадзор

Что такое доступ к информации?
а) возможность получения информации и ее использования;
б) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
в) зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
г) сведения (сообщения, данные) независимо от формы их представления;
д) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

К какой информации МОЖЕТ быть ограничен доступ?

а) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

б) информации о состоянии окружающей среды;

в) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

г) информации о деятельности государственных органов и органов местного самоуправления;

д) государственная тайна.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на (выбрать неправильный ответ):

а) соблюдение конфиденциальности информации ограниченного доступ;

б) реализация права на доступ к информации;

в) обеспечение защиты информации от неправомерного доступа;

г) контроль в области разработки программного обеспечения.

Что не может служить для биометрической идентификации:

а) радужная оболочка глаз;

б) отпечатки пальцев;

в) голос;

г) ключ e-token;

д) подпись

Задания для практических работ представлены в разделе 9.

Вопросы по курсу.

1. Назначение, принципы построения системы защиты информации.
2. Стратегия защиты информации.
3. Основные требования, предъявляемые СЗИ.
4. Методология защиты информации.
5. Методика определения состава защищаемой информации.
6. Классификация информации по видам тайн и степеням конфиденциальности.
7. Определение объектов защиты.
8. Методика выявления способов воздействия на информацию.
9. Причины и условия дестабилизирующего воздействия на информацию.
10. Выявление каналов доступа к информации.
11. Модель потенциального нарушителя.
12. Значение моделирования процессов защиты информации.
13. Архитектурное построение СЗИ.
14. Модель системы автоматизированного проектирования защиты информации.
15. Этапы разработки СЗИ.
16. Состав нормативно-правового обеспечения.
17. Порядок разработки и внедрения документов СЗИ.
18. Понятие и цели управления СЗИ.
19. Планирование деятельности управления СЗИ.
20. Кадровое обеспечение СЗИ.

21. Подбор персонала.
22. Подготовка персонала для работы в новых условиях.
23. Понятие угрозы безопасности компьютерной системы.
24. Методы «взлома» компьютерных систем. Защита компьютерной системы от «взлома». Программные закладки.
25. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
26. Защита программного обеспечения. Превентивные меры защиты.
27. Защита программного обеспечения. Средства собственной защиты.
28. Защита программного обеспечения. Средства защиты в составе вычислительной системы.
29. Защита программного обеспечения. Средства защиты с запросом информации.
30. Защита программного обеспечения. Средства активной защиты.
31. Защита программного обеспечения. Средства пассивной защиты.
32. Технология защиты информации на основе: электронных ключей, смарт-карт, персональных идентификаторов.
33. Принципы и методы создания защищенной операционной системы.
34. Цели и средства защиты информации. Типичный набор функциональных подсистем.
35. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
36. Меры безопасности в контексте ISO 27001.
37. В чем состоит криптографическая задача обеспечения я целостности.
38. Методы идентификации, аутентификации, авторизации пользователей.
39. Классификация методов и средств инженерно-технической защиты информации и объектов информатизации.
40. Методы защиты информации специальными средствами.
41. Принципы управления информационной безопасностью.
42. Стандарты в области менеджмента информационной безопасности.
43. Архитектура систем управления информационной безопасностью.
44. Методы обнаружения инцидентов.
45. Управление инцидентами информационной безопасности.
46. Оценка эффективности реагирования на инциденты.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список литературы

Основная

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2025. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2198501 (дата обращения: 24.06.2025).
2. 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, 2025. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369- 01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2178344 (дата обращения: 24.06.2025).
3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. -

Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566 (дата обращения: 24.06.2025).

Дополнительная

4. Асанов, В. Л. Архитектурный менеджмент и администрирование : учебное пособие для вузов / В. Л. Асанов. — Москва : Издательство Юрайт, 2024. — 202 с. — (Высшее образование). — ISBN 978-5-534-12778-2. — URL : https://urait.ru/bcode/543419.
5. Грибанов, Ю. И. Цифровая трансформация бизнеса : учебное пособие / Ю. И. Грибанов, М. Н. Руденко ; Пермский государственный национальный исследовательский университет. – 2-е изд. – Москва : Дашков и К°, 2021. – 214 с. : ил., схем., табл. – Режим доступа: по подписке. URL: https://biblioclub.ru/index.php?page=book&id=600303 (дата обращения: 26.01.2022). – Библиогр. в кн. – ISBN 978-5-394-04192-1. – Текст : электронный.
6. Зараменских, Е. П. Архитектура предприятия : учебник для вузов / Е. П. Зараменских, Д. В. Кудрявцев, М. Ю. Арзуманян ; под редакцией Е. П. Зараменских. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 436 с. — (Высшее образование). — ISBN 978-5-534-16447-3. — URL : https://urait.ru/bcode/539842
7. Наумов, В. Н. Рынки информационно-коммуникационных технологий и организация продаж : учебник / В. Н. Наумов. — Москва : ИНФРА-М, 2023. — 404 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/21026. - ISBN 978-5-16-012042-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2001668 (дата обращения: 16.06.2025).
8. Глобальные сети : учебно-методическое пособие / М. А. Захаров, А. А. Митьковский, А. Д. Пономарев, А. В. Пролетарский. - Москва : Издательство МГТУ им. Баумана, 2019. - 80 с. - ISBN 978-5-7038-4918-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169186 (дата обращения: 16.06.2025).
9. Основы построения инфокоммуникационных систем и сетей : практикум / сост. А. С. Кольцов, Л. В. Степанов, С. Ю. Кобзистый. - Иваново : ПресСто, 2022. - 80 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1998969 (дата обращения: 16.06.2025).
10. Цифровая экономика : учебник для вузов / И. А. Хасаншин, А. А. Кудряшов, Е. В. Кузьмин [и др.] ; под ред. И. А. Хасаншина. - Москва : Горячая линия - Телеком, 2022. - 287 с. - ISBN 978-5-9912-0791-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2184237 (дата обращения: 16.06.2025).

6.2 Перечень ресурсов информационно-коммуникационной среды “Интернет»

1. Официальный сайт Министерства экономического развития РФ [Электронный ресурс] – URL: http://www.economy.gov.ru (дата обращения 15.05.2025)
2. Федеральная служба государственной статистики https://www.gks.ru/ (дата обращения 15.05.2025)
3. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. – – Москва. – URL: http://elibrary.ru/ (дата обращения 15.05.2025).

6.3 Профессиональные базы данных и информационно-справочные системы
Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7 Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимы:

- *для лекций:*
- учебная аудитория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук,
- программное обеспечение (ПО).

- *для практических занятий:*
- лаборатория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук для преподавателя,
- компьютеры для обучающихся,
- выход в Интернет,
- программное обеспечение (ПО).

Перечень программного обеспечения (ПО)

- *для лекций:*

№п/п	Наименование ПО	Способ распространения
1	Microsoft Office 2010 Pro	лицензионное
2	Windows 10	лицензионное
3	Kaspersky Endpoint Security	лицензионное

- *для практических занятий:*

Наименование ПО	Способ распространения
Windows 10	лицензионное
Microsoft Office 2010 Pro	лицензионное
Mozilla Firefox	свободно распространяемое
Kaspersky Endpoint Security	лицензионное
Microsoft SQL Server 2008	лицензионное
Microsoft Visual Professional 2019	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: Основы криптографии

Одним из методов защиты конфиденциальности информации является криптография.

- Перечислите основные методы криптографической защиты информации.
- Перечислите недостатки и преимущества симметричных и асимметричных криптосистем.
- В каком случае метод гаммирования дает абсолютную криптостойкость?

Типовые задания:

1. Расшифровать, используя таблицу Виженера следующую криптограмму:

а) Ключ: АМЕРИКА

Шифрограмма:
МЗФДЙЦИКАЙЭШЩДБЫХЫЬУЗВЗЦЫИТЫВМТЩТЬДЕШЕЮЦЁХВЮЖЯНМРЕЩД ТЪЩВЕЭЭХЦШОССХМНТНОЦ ЩЯЩЧЕ

(Исходный текст: мы публикуем подборку из высказываний сделанных в свое время в совершенно серьезной форме)

б) Ключ: ЕВРОПА

Шифрограмма:
ИВНБЮБАНЯАЪАМВЮЭСПУНЮУБЕХЮХЦЭОНРСЭБНУДРЬЭОИНПАСОЙЕЯРАЕС ЖЮЧ

(Исходный текст: да это было сказано вполне серьезно и обоснованно для своего времени)

в) Ключ: АЗИЯ

Шифрограмма:ИХЫДРМЪМОЗАСОИЬГЕЪКЪЗГКЯТДЬМАЩЬКЫИУТИПЫНГЦАСОК ЧБОШСССЖЪДГЦМ МЯ

(Исходный текст: интересно а что будет вызывать у нас улыбку из того что говорится сегодня)

Тема 2: Технологии использования электронной подписи

Вопросы

Одним из реквизитов электронного документа является электронная подпись (ЭП).

- Какова технология получения ЭП?
- Что такое сертификат ЭП?
- Что обеспечивается с помощью ЭП?
- Виды электронных подписей.
- Сфера применения каждого вида ЭП.
- Госключ – сфера применения, технологии использования.
- МЧД – сфера применения, технологии использования.

Тема 3: Кадровый электронный документооборот (КЭДО)

Вопросы

- Нормативная база перехода на КЭДО.
- Виды документов, включаемые в КЭДО.
- Какие документы не включаются в КЭДО?

- Программно-техническое обеспечение КЭДО.
- Организационное обеспечение КЭДО.
- Электронный архив – нормативно-правовая база.
- Электронный архив – специфика реализации.

Тема 4: Определение и нормативное закрепление состава защищаемой информации
Вопросы
- Какими факторами определяется состав угроз защищаемой информации.
- Какова процедура выявления каналов несанкционированного доступа к информации на предприятии?
- Чем определяется состав нарушителей и как осуществляется их категорирование?
- Как может проводиться оценка степени уязвимости информации в результате действий нарушителей различных категорий?

9.2 Методические рекомендации по подготовке письменных работ

Отчет по проделанной работе должен быть изложен с соблюдением правил грамматики русского и английского языков (в случаях необходимости). При этом отражаемые результаты работы должны быть информативными, тезисного порядка. В отчет входят следующие обязательные разделы:

1. Титульный лист с полным указанием ведомственной принадлежности, названия ВУЗа, института, факультета, кафедры. Кроме того, полное точное название лабораторной работы, Ф.И.О. студента, подготовившего отчет о результатах проделанной работы и Ф.И.О., должность, название кафедры преподавателя, осуществляющего проверку и оценивание полученных результатов.
2. Содержание.
3. Введение.
4. Цели и задачи практической работы.
5. Методы и технологии, применяемые для решения поставленных задач оформленные в виде отдельных этапов работы.
6. Выводы по работе.
7. Приложения.

Оформление отчета выполняется с использованием компьютерной верстки LaTeX. Отчет сохраняется и представляет для проверки в виде отдельного pdf файла. В имени файла показывается фамилия студента и номер выполненной работы.