Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.07 «МЕДОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: Магистратура
Форма обучения: очная

Королев
2023

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Автор: Сухотерин А.И. Рабочая программа дисциплины (модуля): Методы и средства защиты информации в системах электронного документооборота. – Королев МО: «Технологический Университет», 2023

Рецензент: Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н., к.в.н., доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является:

- умение эффективно использовать методы моделирования на практике. формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации в СЭДО;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации в СЭДО, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Общепрофессиональные компетенции:

- ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.
- ОПК-3: Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.

Основными задачами дисциплины являются:

Научить обучаемых самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации и формированием у обучающихся системы знаний, умений и навыков по защите информации, обеспечению информационной безопасности граждан, общества и государства. В том числе:

- построение разрешительной системы доступа к конфиденциальной информации;
- определение номенклатуры дел, формирование и оформление конфиденциальных дел;
- разносторонний обзор систем электронного документооборота;
- раскрытие общих положений по защите информации в СЭД;
- научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации с СЭД;

- ознакомить студентов при решении поставленных задач с помощью перспективных технологий и методов защиты информации;
- ознакомить студентов с методикой применения и использования встроенных механизмов защиты информации;
- ознакомить студентов с порядком применения средств добавочной защиты информации.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- ОПК-1.3. Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении.
- ОПК-3.3. Применяет отечественные стандарты при сертификации средств защиты и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки организационно-распорядительных документов.

Необходимые умения:

- ОПК-1.2. Проектирует системы и подсистемы ИБ с учетом современных безопасных инструментальных технологий.
- ОПК-3.2. Разрабатывает технические задания на создание подсистем обеспечения информационной безопасности.

Необходимые знания:

- ОПК-1.1. Формирует актуальные модели угроз и нарушителей для современных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности.
- ОПК-3.1. Исследует и проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Методы и средства защиты информации в системах электронного документооборота» Б1.О.07 относится к обязательной части блока 1 основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина базируется на ранее изученных дисциплинах: “Экономика и управление”, “Защищенные информационные системы”, ”Основы теории информационной безопасности“, «Методы и средства обеспечения безопасного доступа к информационным ресурсам» и компетенциях УК-1, 2; ОПК-1; ПК-1, 2, 3;.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин «Информационно-аналитические системы безопасности», «Информационная безопасность финансово-кредитных структур», «Компьютерное моделирование информационных процессов и технологий» прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины представлена в таблице 1 и составляет 2 зачетные единицы, 72 часа. Дисциплина читается на 2 курсе в 3-ем семестре.

Таблица 1

Виды занятий	Всего часов	Семестр 3
Общая трудоемкость	**72**	**72**
Аудиторные занятия	**46**	**46**
Лекции (Л)	16	16
Практические занятия (ПЗ)	12	12
Лабораторные работы (ЛР) и (или) другие виды аудиторных занятий	12	12
Другие виды контактной работы*	**6**	**6**
Практическая подготовка	**4**	**4**
Самостоятельная работа	**24**	**24**
Расчетно-графические работы	-	-
Контрольная работа, домашнее задание	-	-
Текущий контроль знаний	тест	тест
Вид итогового контроля	экзамен	экзамен

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Темы дисциплины и виды занятий

Темы дисциплины, количество часов на лекции и практические занятия приведены в таблице 2.

Таблица 2

Наименование тем	**Лекции, час.**	**Практ. занятия, час**	**Лаб. занятия час**	**В интерак. форме**	**Практическая подготовка**	**Код компетенций**
Тема 1: Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации	4	3	3	1	**1**	ОПК-1
Тема 2: Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации. Составление номенклатуры дел, формирование и оформление конфиденциальных дел	4	3	3	1	1	ОПК-1
Тема 3: Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации	4	3	3	2	1	ОПК-1 ОПК-3
Тема 4: Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота.	4	3	3	2	1	ОПК-1 ОПК-3
Итого:	**16**	**12**	12	6	4	

5.2. Содержание тем дисциплины

Тема 1: Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации

Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Общие положения. Персональные данные. Тайна следствия и судопроизводства. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Секрет производства (ноу-хау) и служебный секрет производства. Документирование конфиденциальной информации.

Особенности документирования конфиденциальной информации. Определение степени ограничения доступа к документам и использование отметки конфиденциальности при оформлении документов. Разработка Перечня конфиденциальной документированной информации. Учёт бумажных носителей конфиденциальной информации. Учёт проектов конфиденциальной документированной информации. Особенности создания и изготовления конфиденциальных документов с помощью средств электронно-вычислительной техники, их печатания, тиражирования, размножения. Учёт использования и хранения печатей, штампов, бланков, необходимых для оформления конфиденциальных документов.

Тема 2: Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации. Составление номенклатуры дел, формирование и оформление конфиденциальных дел

Особенности учёта и регистрации конфиденциальной документированный информации. Обработка поступающих конфиденциальных документов, их учёт и регистрация. Учёт и регистрация внутренних (созданных/изданных) конфиденциальных документов. Технологии исполнения и контроля за исполнением конфиденциальных документов. Учёт и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка. Учёт конфиденциальной документированной информации инвентарного (выделенного) хранения. Учёт конфиденциальной информации при ее автоматизированной обработке.

Основные требования к разрешительной системе документа. Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства. Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти. Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные. Особенности доступа к архивным конфиденциальным документам. Особенности доступа

должностных лиц при их командировании к конфиденциальной документированной информации. Учёт персонала, получившего доступ к конфиденциальной документированной информации, и (или) лиц, которым она была передана или предоставлена. Документальный фонд организации. Формирование конфиденциальных дел. Оформление конфиденциальных дел.

Тема 3: Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации

Экспертиза ценности конфиденциальных документов. Подготовка конфиденциальных документов и дел для архивного хранения. Подготовка конфиденциальных документов и дел к уничтожению.

Режим обмена конфиденциальной документированной информацией. Режим сохранности конфиденциальных документов и дел. Режим конфиденциальности при проведении совещаний и переговоров. Проверка наличия носителей конфиденциальной информации.

Тема 4: Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота.

Особенности конфиденциального электронного документооборота. Основные виды угроз информационной безопасности организации. Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе. Организация работ при создании системы защиты электронного документооборота. Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке. Обеспечение контроля защиты электронного документооборота. Аттестация автоматизированных информационных систем по требования безопасности информации. Защита от вредоносных программ. Защита системы электронных сообщений.

Основные требования к системам электронного документооборота. Краткая характеристика систем электронного документооборота.

Обобщенные требования к функционированию ЭДО. Декомпозиция задачи построения СЭД. Создание УЦ. Функции центра сертификации (ЦС). Механизмы защиты СЭДО. СМЭВ (система межведомственного электронного взаимодействия) как ее применять в системах ЭДО. Характеристика системы ЭДО «Канцлер», «Бюрократ», «Алтиус». Сокращение издержек при переходе на ЭДО: практические шаги. Цели проекта. Границы проекта. Ограничения и риски проекта. Рабочая группа. Выбор программной платформы. План проекта.

5.Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю).

«Методические указания для обучающихся по освоению дисциплины (модуля)» представлены в Приложении 2 к настоящей РП.

6.Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине (модулю) «Методы и средства защиты информации в системах электронного документооборота » приведена в Приложении 1 к настоящей РП.

7.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

4.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

5.Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

6.Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

7.Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

8.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

8.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины (модуля)

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+, Гарант.).

Лабораторные работы:

- компьютерная аудитория, оснащенная программно-аппаратными средствами защиты информации и аудита компьютерной безопасности, а также оснащенная специализированным оборудованием и контрольно-измерительной аппаратурой.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Задания.

ЗАДАНИЕ

Тема: *Обеспечение безопасности информации в системах электронного документооборота*

Цель занятия: *Приобретение студентами теоретических знаний области организации систем электронного документооборота, а также формирование профессиональных компетенций, необходимых для реализации методов и средств защиты информации в подобных системах*.

Продолжительность занятия – *2 ак.ч.*

Задание –

1. Провести сравнительный анализ возможностей защиты информации представленных в приложении 1 систем электронного документооборота;

2. По итогам анализа заполнить таблицу возможностей защиты информации СЭД, пример таблицы представлен в приложении 2.

3. Выбрать программный продукт СЭД для внедрения в организацию, обосновать свой выбор;

4. Разработать комплекс мер для обеспечения информационной безопасности СЭД организации, включающий:

А) Организационные меры;

Б) Программные меры;

В) Технические меры.

5. Представить отчет по выполненным п.1-п.4.

Справочная информация представлена в Приложениях к лабораторной работе.

Приложение 1

В настоящее время системы электронного документооборота (СЭД) становятся обязательным элементом ИТ-инфраструктуры любой организации. С их помощью коммерческие предприятия повышают эффективность своей деятельности, а в государственных учреждениях на базе систем электронного документооборота решаются задачи внутреннего управления, межведомственного взаимодействия и работы с обращениями граждан.

Система электронного документооборота – это система автоматизации работы с информационными документами на протяжении всего их жизненного цикла (создание, изменение, хранение, поиск, классификация и пр.), а также процессов взаимодействия между сотрудниками.

В СЭД обрабатывается большое количество информации конфиденциального характера, поэтому формирование защищенного документооборота становится актуальной задачей для любой компании. Необходимо обеспечивать защиту документов и обеспечивающих компонентов СЭД от предумышленных и случайных угроз информационной безопасности.

Особенности защиты данных в СЭД.

Среди угроз для систем электронного документооборота можно выделить следующие:

– угроза целостности

– уничтожение или искажение информации, которое может быть как непреднамеренным, так и умышленным;

– угроза конфиденциальности – любое нарушение конфиденциальности, при котором информация становится известной лицам, не имеющим к ней доступ (кража, перехват информации);

– угроза доступности – угроза, нарушающая возможность получить своевременный и беспрепятственный доступ к информации пользователям, имеющим к ней права доступа;

– угроза работоспособности системы – угроза, реализация которой приводит к сбою в работе системы; – невозможность доказательства авторства – угроза, выражающаяся в том, что если в документообороте не используется электронная подпись, то невозможно доказать, что именно данный пользователь создал данный документ, при этом невозможно сделать документооборот юридически значимым.

Обеспечение защиты данных именно от этих угроз является задачей, которую в той или иной мере должна выполнять система электронного документооборота. В любой СЭД необходимо реализовать механизмы защиты от основных угроз: контроль доступа и разграничение прав пользователей, обеспечение сохранности и подлинности документов, протоколирование действия пользователей.

В целях обеспечения сохранности документов и возможности их быстрого восстановления в системе должна быть реализована функция резервного копирования. СЭД, которые используют базы данных Microsoft SQL Server или Oracle и др., чаще всего выбирают средства резервного копирования от

разработчика СУБД. Другие используют собственные подсистемы резервного копирования, разработанные непосредственно производителем СЭД.

Для защиты СЭД от угроз информационной безопасности необходимо обеспечить безопасный доступ к системе, то есть должны быть реализованы механизмы аутентификации пользователей и разграничение прав доступа. Классика удостоверения личности в информационных системах – пароль. Однако данный метод аутентификации небезопасен. Следующий метод – имущественный, когда для аутентификации могут быть использованы USB-ключи, смарт-карты и т. п. Максимально надежный для проведения идентификации и последующей аутентификации способ – биометрический. При использовании данного метода человек идентифицируется по своим биометрическим данным (голос, отпечаток пальца, сканирование сетчатки глаз). Однако в данном случае возрастает стоимость решения, к тому же технологии считывания этих показателей еще не настолько совершенны, чтобы избежать ошибок или отказов. Еще один важный аспект аутентификации – это его многофакторность. Идея многофакторной аутентификации заключается в том, чтобы взаимно компенсировать недостатки нескольких отдельных факторов. Возможно комбинирование различных методов: парольного, имущественного и биометрического. На практике чаще всего используется двухфакторная аутентификация, например, аутентификация при помощи пароля и отпечатка пальца.

Для разграничения прав доступа в СЭД обычно используется подсистема СЭД, созданная разработчиками, или используется подсистема безопасности, реализованная в СУБД, которая применяется в СЭД.

Конфиденциальность документов, обрабатываемых в СЭД, должна обеспечиваться криптографическими методами защиты информации. Благодаря им сохраняется конфиденциальность информации, даже в случае попадания посторонним лицам. Однако любой криптографический алгоритм обладает своим уровнем криптостойкости, поэтому нет таких шифров, которые нельзя взломать, это всего лишь вопрос времени и средств.

На сегодняшний день основным решением для обеспечения подлинности документа является электронная цифровая подпись (ЭЦП), принцип работы которой основан на шифровании с ассиметричным ключом. Электронная подпись наделена юридической силой наряду с собственноручной подписью в соответствии с ФЗ-63 «Об электронной подписи». Согласно законодательству Российской Федерации, свою систему электронной подписи может разрабатывать только компания, которая имеет на это соответствующую лицензию ФСБ.

Протоколирование действий пользователей в системах – один из важнейших аспектов в защите электронного документооборота. Так как все действия пользователей регистрируются, то при возникновении проблем можно найти виновника, а также пресечь попытку неправомерных действий.

Платформа Docsvision является базисом для электронного документооборота и позволяет реализовать самые разнообразные решения в области

автоматизации бизнес-процессов и задач обработки документов. Платформа состоит из клиентской и серверной части. Конструкторы, модули, шлюзы к другим системам и готовые приложения Docsvision позволяют гибко настроить систему под решение конкретных бизнес-задач заказчика.

Защита информации в Docsvision реализована: мандатным управлением доступа, разграничением прав доступа на всех уровнях, настройкой передачи прав, протоколированием и регистрацией действий пользователя, применением шифрования. Реализована поддержка электронной подписи всех трех видов, предусмотренных российским законодательством (№ 63-ФЗ). Имеет сертификат ФСТЭК.

Интеграция Docsvision с решением SafeCopy компании «НИИ СОКБ» позволяет предотвратить распространение конфиденциальных документов, которые хранятся в Docsvision, и избежать несанкционированной передачи таких документов посторонним лицам. Данная интеграция позволяет решать следующие задачи: защита конфиденциальных документов и документов, составляющих коммерческую тайну, выявление злоумышленников в случае возникновения инцидента, централизованный контроль за распространением печатных и электронных копий конфиденциальных документов.

Пользователями СЭД Docsvision являются: РКЦ «Прогресс», ЗАО «Центр Финансовых Технологий», администрация Екатеринбурга, страховая компания «Райффайзен Лайф», автозавод «ГАЗ», Мосгоризбирком, Министерство экономического развития РФ, «Газпром добыча Краснодар».

Система «ДЕЛО», разработанная компанией «Электронные Офисные Системы», поддерживает работу с документами на всех этапах жизненного цикла. Система обеспечивает регистрацию, рассмотрение, выдачу поручений, работу с проектами резолюций, контроль исполнения поручений и мониторинг сроков исполнения, списание документов.

Защита информации в СЭД «ДЕЛО» реализована функциями ЭЦП и шифрования. Подписание электронной подписью и ее проверка в СЭД «ДЕЛО» реализуется через опции «ЭП и шифрование» и «Сервер удаленной проверки ЭП». Поддерживается работа с сертифицированными средствами криптографической защиты информации. Шифрование сообщений, передаваемых по открытым каналам, позволяет защитить конфиденциальную информацию от несанкционированного доступа.

Задача обеспечения безопасности данных решена с помощью Secret Disk Server NG компании Aladdin – системы защиты корпоративных баз и конфиденциальной информации на серверах от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия. Для авторизации пользователей в системе «ДЕЛО» используется программно-аппаратный комплекс «Мастер паролей». Логины и пароли хранятся на специальной смарткарте, доступ к которой можно закрыть PIN-кодом.

СЭД «ДЕЛО» включена в Реестр отечественного ПО. СЭД «ДЕЛО» используется как в государственных организациях, так и в коммерческих компаниях. На базе системы электронного документооборота «ДЕЛО» осу-

ществляется предоставление государственных и муниципальных услуг в электронном виде на федеральном, региональном и муниципальном уровнях. Это обеспечивается интеграцией с «Единым порталом государственных и муниципальных услуг» (ФГИС ЕПГУ) и Системой межведомственного электронного взаимодействия (СМЭВ).

Пользователями СЭД «ДЕЛО» являются: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Арбитражные суды, Генеральная прокуратура Российской Федерации, Центральный банк Российской Федерации, ГФС России, Росархив, Минтруд России.

CompanyMedia – корпоративная система управления документами, задачами и личной продуктивностью. Выполняя функции делопроизводства, система также сфокусирована на работе руководителей и бизнес-специалистов. CompanyMedia имеет 4-уровневую структуру: уровень технологической платформы, уровень базовых сервисов, уровень прикладных модулей и уровень представления информации. СЭД CompanyMedia обеспечивают защиту информации и юридическую значимость электронных документов.

Задачи защиты информации решаются благодаря следующим возможностям CompanyMedia:

– эффективное разграничение прав доступа пользователей к данным и различным частям системы в зависимости от служебного положения;

– авторизованный доступ к ресурсам системы за счет надежной идентификации и аутентификации;

– регистрация событий безопасности, связанных с действиями пользователей и администраторов;

– применение сервиса Locker, позволяющего обеспечить целостность информации в системе за счет использования электронной подписи (ЭП), в том числе усиленной.

Имеет сертификат ФСТЭК.

Пользователями CompanyMedia являются: Банк ВТБ, ОАО «Россельхозбанк», ОАО «Газпромбанк», УРАЛСИБ, Корпорация «Комета», правительство Омской области, правительство Новосибирской области, правительство Севастополя, АО «НПП «ЗВЕЗДА».

«Е1 Евфрат» – система электронного документооборота, используется для автоматизации процессов делопроизводства, организации корпоративного документооборота, автоматизации типовых бизнес-процессов для компаний всех типов и размеров. СЭД «Е1 Евфрат» использует в качестве платформы собственную разработку компании – CognitiveNexus, основными СУБД – MS SQL Server, MySQL, Oracle, также возможна реализация проектов и на других СУБД. «Е1 Евфрат» разработан в соответствии требованиям стандарта ISO 9000.

«Е1 Евфрат» включает в себя модуль информационной безопасности, который соответствует требованиям в области защиты информации. Модуль

реализует комплексную защиту данных как от внешнего, так и от внутреннего несанкционированного доступа и обеспечивает сохранность и целостность документов в случае технических сбоев и аварий. «Е1 Евфрат» поддерживает использование протокола SSL для шифрования, расширенную квалифицированную электронную подпись КриптоПро и других сертифицированных криптопровайдеров, доменную авторизацию. Реализован механизм разграничения прав доступа. Хранение и управление паролями осуществляется средствами ОС, пароли никогда не передаются по сети в открытом виде. В СЭД «Е1 Евфрат» ведутся отдельные списки пользователей, имеющих права на регистрацию, контроль за прохождением документов, создание шаблонов отчетов и журналов, доступ к любым документам на чтение и изменение, а также администрирование системы. Наличие сертификатов ФСТЭК и ФСБ.

Пользователями «Е1 Евфрат» являются: ОАО «РЖД Логистика», ЭКООФИС, Государственное учреждение «Московское объединение ветеринарии», администрация главы и правительства Чеченской Республики, г. Грозный; ОАО «Коммерческий банк КЫРГЫЗСТАН».

Система «Логика СЭД» предназначена для автоматизации управленческого документооборота и делопроизводства, а также управления бизнес-процессами в средних и крупных коммерческих и государственных предприятиях.

Система «Логика СЭД» включена в реестр отечественного ПО и использует для работы СУБД PostgresPro. Имеет сертификат ФСТЭК. В «Логику СЭД» встроена поддержка сертифицированных ФСБ России средств криптографической защиты информации.

В системе используются следующие механизмы защиты данных:

– электронная подпись;

– разграничение прав доступа пользователей;

– протоколирование действия пользователей;

– шифрование данных.

Для реализации функций криптографической защиты информации используется программный продукт «Логика ECM. Штамп». Его преимуществами является: кроссплатформенность, кроссбраузерность, соответствие законодательства РФ, обеспечение юридической значимости электронных документов, конфиденциальность информации и контроля ее целостности.

Пользователями «Логика СЭД» являются: Федеральная налоговая служба РФ, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральное агентство по управлению особыми экономическими зонами, Федеральное агентство лесного хозяйства, Федеральное агентство водных ресурсов, Министерство природных ресурсов, Министерство юстиции РФ.

Приложение 2

Результаты анализа возможностей защиты информации в исследуемых СЭД представлены в таблице:

«+» – возможность реализована;

«+/−» – возможность доступна в рамках ограниченной функциональности или требуется приобретение дополнительного ПО;

«−» – возможность не реализована.

Защита информации	**ДЕЛО**	**Логика СЭД**	**Docvision**	**Е1 Евфрат**	**Companymedia**
Поддержка различных способов аутентификации					
Назначение прав пользователям					
Назначение прав группам пользователей					
Поддержка пользовательских ролей					
Выдача прав на время исполнения документа					
Шифрование данных системы, шифрование данных при передаче					
Средства мониторинга событий в системе					
Использование ЭЦП					
Применение сертифицированных средств защиты					
Протоколирование действий пользователя					
Организация резервного копирования базы данных					

ЗАДАНИЕ
Тема: Описание и реализация документооборота в организации: применение СЗИ для защиты и безопасного изолирования компонентов документооборота

1. Изучить предлагаемый подход.
2. Разработать собственную структурно-функциональную схему ЗЭДО предприятия (организации). Предназначение всех компонентов.

Компоненты системы электронного документооборота и их функции

Система электронного документооборота в компании должна содержать следующие элементы:

- модуль электронного делопроизводства (регистрация входящих/исходящих документов);
- модуль электронного архива со средствами поиска документов и комплектом шаблонов документов;
- модуль WorkFlow - электронное движение и согласование документов;
- модуль сквозного контроля исполнения поручений;
- модуль информационно-защищенного обмена документами между юридическими лицами и/или удаленными филиалами;
- модуль генерации отчетов о движении документов;
- модуль коллективной работы с документами.

Если же система электронного документооборота также применяется для автоматизации процессов управления, то добавляются:

- модуль на основе WorkFlow для планирования, управления и мониторинга за ходом процессов;
- модуль развернутой аналитики и план/фактного выполнения процессов.

Система автоматизации документооборота складывается из нескольких подсистем. Каждая подсистема обладает набором специфических для нее функций. При этом отдельные подсистемы тесно взаимодействуют между собой. Разделение системы документооборота на подсистемы, предпринимаемое нами, носит несколько “академический” характер. В реальной практике программные продукты достаточно условно можно отнести к той или иной группе в нашей классификации. Как правило, системы реализуют лишь часть функций, описанных ниже, при этом продукт одного класса может включать в себя часть функций систем другого класса.

Можно выделить следующие **подсистемы автоматизации документооборота**:

- подсистема автоматизации делопроизводства;
- архивы документов;
- подсистема ввода документов и обработки образов документов;
- подсистема управления стоимостью хранения документов;

- подсистема маршрутизации документов;
- подсистема комплексной автоматизации бизнес-процессов.

Подсистема автоматизации делопроизводства

Функции автоматизации делопроизводства в том или ином виде представлены в любой системе автоматизации документооборота. В функции **систем автоматизации делопроизводства** не входит хранение и перемещение документов в организации. В их функции входит **фиксация документов** в специальной базе данных, выражающаяся в заполнении специальной карточки документа. Содержимое карточки документа может варьироваться в зависимости от сложившейся в организации ситуации. Структура документов, зафиксированных в базе данных, опирается на так называемую номенклатуру дел, имеющуюся, как правило, в каждой организации, а технология учета и обработки документов опирается на сформулированное в данной организации “Положение о делопроизводстве”.

Документы хранятся в бумажном виде, в специальном архиве, но в базе данных отображается их текущее местоположение и статус, включая атрибуты контроля исполнения. Обычно в системах делопроизводства различают входящие и исходящие документы, нормативно-распорядительные документы, документы коллегиальных органов управления, справочные документы и пр. Документы, находящиеся на контроле исполнения, подразделяются по исполнителям, статусу исполнения, срокам исполнения и прочее. Каждый документ в системе представляет собой запись в базе данных, характеризующуюся набором значений атрибутов карточки. Помимо учета и поиска документов в базе данных, система должна обеспечивать генерацию отчетов, позволяющих получить ведомости исполнения документов и прочую сводную информацию.

Однако в том случае, если автоматизация документооборота не закончится данным шагом, то можно подумать и о других инструментах, обеспечивающих более последовательное развитие системы. Так, например, при переходе к электронному хранилищу документов база данных системы делопроизводства должна содержать ссылки на соответствующие объекты электронного архива, при использовании электронных средств маршрутизации документов система должна обеспечивать возможность рассылки документов на рабочие места пользователей, определения текущего местоположения документа и так далее.

Архивы документов

Подсистема архивации документов управляет архивами документов. Архив документов – это то, что собственно хранит электронный документ. При этом может храниться либо образ документа, либо его содержание, либо и то и другое. Помимо собственно **хранения документов**, архив должен обеспечивать **навигацию по иерархии документов** и их поиск.

В отличие от поиска по атрибутам документов, который имелся и в системах предыдущего класса, архивы документы должны обеспечивать **полнотекстовый поиск по содержимому текстовых фрагментов** в до-

кументе. В предельном случае поисковый механизм должен обладать некоторым интеллектом, то есть обеспечивать поиск близких грамматических конструкций, а также поиск близких по смыслу слов.

В отличие от систем предыдущего класса, в архивах хранятся сами документы, и поэтому система должна обеспечивать **разграничение прав доступа** к документам. Пользователь может идентифицироваться либо посредством сетевого имени, либо с помощью специального имени и пароля, определенного в системе управления архивом. Помимо разделения прав доступа на уровне пользователей система должна обеспечивать **выделение групп пользователей или ролей**.

Следующей функцией архива документов является **обеспечение возможности групповой работы** с документами, находящимися в стадии создания - это функция **блокировок документов** или Check-In/Check-Out контроль. Если один из пользователей системы начинает редактировать документ, он блокируется для доступа других пользователей до тех пор, пока с ним не закончится работа.

Еще одной функцией архива является **поддержка контроля версий**. Версии документов могут фиксироваться либо автоматически, либо по инициативе пользователя. В случае необходимости пользователь может вернуться к одной из предыдущих версий документа.

К сервисным функциям архива документов относятся возможность **создания резервных копий документов** без прекращения работы системы, интеграция с системами обеспечения оптимальной стоимости хранения данных и прочее.

Подсистема ввода документов и обработки образов документов выполняет **ввод документов в архив**. Под этим понимается перевод документов из бумажного вида в электронный. В простейшем случае эта процедура сводится к простому сканированию. Однако, как правило, простого сохранения образа документа оказывается недостаточно.

Образ документа может потребовать так называемого аннотирования, наложения на образ документа различных дополнительных образов, выделений, текстовых пометок и прочее. Помимо этого, образ документа должен быть снабжен набором атрибутов, который позволит его идентифицировать в системе делопроизводства и в архиве документов. Эти операции производятся вручную.

Более сложной функцией является **автоматическое распознавание содержимого** образа документа и **формирование документа**, содержащего его текст. Для этого предназначены программы, относящиеся к классу ПО распознавания текста. Еще более сложной функцией является **распознавание содержимого форм**. При этом программа определяет наличие записей, в том числе и рукописных в определенных полях бланка документа, распознает его содержимое и автоматически заполняет значения атрибутов данного документа в системе. При необходимости значения опре-

деленных полей бланка может выбираться из определенного в системе справочника.

Дополнительно:

Перевод бумажных документов в электронную форму

Данная проблема подразделяется на два основных класса:

Персональный ввод бумажных документов. Ввод небольшого количества разнотипных бумажных документов осуществляется с помощью планшетных или персональных сканеров. После операции сканирования документ вручную индексируется путем заполнения карточки документа.

Массовый (поточный) ввод бумажных документов. Основное отличие от предыдущего состоит в том, что обрабатывается большое количество однотипных документов. В качестве примеров приложений данной технологии в конкретных предметных областях можно привести: систему ввода и хранения платежных поручений в банке, систему обработки анкет опроса населения, систему обработки результатов голосования.

При реализации технологии массового ввода документов можно рассматривать два основных класса задач:

1) Задача извлечения данных из бумажных документов. Например, имеется форма с результатами опроса населения. Необходимо ввести большое количество анкет, извлечь из них данные и загрузить в некоторую базу. В этом случае нас интересуют только извлеченные структурированные данные, а не сами изображения документов.

2) Задача извлечения данных из бумажных документов с сохранением изображения документа. Если вы обрабатываете не форму с опросами населения, а платежное поручение клиента, то имеет смысл после извлечения данных сохранить изображение документа для того случая, когда потребуется анализ исходного документа. Извлеченные данные можно опять-таки использовать двояко. Во-первых, эти данные имеет смысл напрямую загружать в банковскую систему, а, во-вторых, их можно использовать для организации хранения и быстрого поиска изображений платежных поручений. В случае применения извлеченных данных для индексирования изображения документа необходимо разделять типы извлеченных данных. В основном на выходе используются структурированные данные, и тогда для поиска применяется атрибутивная индексация, но бывают случаи, когда из документа извлекаются только неструктурированные данные (например при распознавании всего содержимого документа). Тогда требуется полнотекстовая индексация. Возможна также и промежуточная задача, когда сохраняется не все изображение, а только его часть, допустим подпись клиента на чеке или платежном поручении.

Работа системы массового ввода разбивается на две основные части - подготовка обработки документа и собственно обработка.

Подготовка обработки документа

Чтобы начать работать с каким-либо документом, необходимо описать его для использования в системе, а именно создать и зарегистрировать новый

класс документа. При этом первым шагом должно быть получение отсканированного изображения незаполненного документа и создание формы по отсканированному шаблону в том случае, если мы регистрируем уже кем-то разработанный документ, либо создание формы для нового документа.

После этого с помощью специального программного модуля (Редактор Форм) требуется определить те поля, которые будут распознаваться системой или заполняться оператором с клавиатуры, а также указать типы данных обрабатываемых полей документа. Для распознаваемых полей следует определить специальные атрибуты модуля с целью повышения точности распознавания, например наличие рукописных цифр, которые находятся в специальных рамках, или символов, напечатанных на машинке. Также можно задать специальные правила проверки корректности обрабатываемых полей документа.

Для конкретного класса документа можно создать несколько форм ввода, используемых либо при редактировании неправильно распознанных данных, либо при ручном вводе полей документа. Возможность создания нескольких форм ввода позволяет назначать для конкретного пользователя конкретные поля для редактирования, что значительно повышает его производительность. Например, в документе имеется рукописное поле, которое не подлежит распознаванию. Создается форма ввода, где есть только одно это поле. Оператор осуществляет ввод только данного конкретного поля, что значительно увеличивает производительность за счет появления в его работе элементов автоматизма.

Для конкретного класса документа, с помощью Редактора Модели Ввода, можно разработать специфичную модель обработки документа, которая определяет операции обработки конкретной копии документа.

Также процесс подготовки документа к вводу в систему необходимо дополнить настройками экспорта документа (Редактор Экспорта) в архивную систему. Данная настройка заключается в установке соответствия между полями формы документа (распознанными или введенными вручную) и полями карточки документа архивной системы. Немаловажной особенностью является способность модуля настройки привязывать содержимое поля документа к проверке на вхождение в справочники архивной системы. Например, если в Редакторе Форм было описано поле "Номер клиента" и к нему прикреплен конкретный справочник системы управления документами, а в процессе ввода был распознан номер, которого нет в этом справочнике, следовательно, возникла исключительная ситуация, которую можно решать двумя методами -или повторно обработать документ, или ввести новый номер в справочник.

После регистрации нового класса документа система готова к работе с реальными документами, предназначенными для сканирования.

Обработка документа

Одной из возможностей повышения эффективности системы ввода документов является предварительная подготовка документов для сканирования. Перед сканированием необходимо отсортировать документы различных

классов и сформировать пакеты документов. Каждый пакет может сопровождаться специальным титульным листом с кодом идентификации данного пакета. Это позволяет одновременно сканировать пакеты с документами разных классов без дополнительных задержек.

После сканирования документы автоматически направляются на операцию распознавания, непосредственно перед которым система осуществляет ряд операций, улучшающих изображение, а значит, и точность распознавания. Выполняются такие операции, как выравнивание, удаление шума и линий, восстановление символов и др. Система может распознавать печатный текст, рукописные цифры и специальные отметки. Также возможно одновременное использование нескольких распознающих модулей. При этом, безусловно, теряется скорость, но точность распознавания значительно повышается. Очень важно сказать, что при этом значительно понижается возможность пропуска некорректных данных. В зависимости от результатов распознавания, поле помечается как корректное или некорректное. Для повышения надежности данных после распознавания применяются определенные пользователем правила проверки данных. Например, можно проверить, имеется ли распознанная информация в вашей базе данных. Если данные после распознавания помечены как некорректные, то они автоматически направляются на ручное редактирование. Во время редактирования оператор видит реальное изображение нераспознанного поля и имеет возможность откорректировать его. После ввода оператором новых данных опять-таки применяются правила проверки данных - на всех этапах ввода, как автоматического, так и ручного, осуществляется проверка данных в соответствии с правилами, определенными пользователем. После извлечения данных из документа необходимо провести операцию экспорта документов и извлеченной информации в систему управления документами.

В результате выполнения всех этих операций документы заносятся в архив и становятся доступными для всех сотрудников предприятия. Необходимо отметить, что на каждом этапе обработки документов может использоваться произвольное количество станций (серверов) обработки.

Важную роль в системе электронного документооборота играет подсистема **управления стоимостью хранения документов**. Совершенно очевидно, что при сохранении в архиве образов документов объемы хранения могут быстро расти и достигать значительных объемов. При этом интенсивность обращения к документам, находящимся в архиве далеко не равномерна. Документы, находящиеся в работе, очевидно, требуются достаточно часто, в то время как доступ к документам, работа с которыми уже завершена, осуществляется очень редко. Соответственно, система может **обеспечивать различную оперативность доступа** к различным документам. Так как стоимость хранения документов в архиве, как правило, обратно пропорциональна скорости доступа, то можно воспользоваться отмеченной закономерностью для оптимизации стоимости содержания архива.

Системы управления стоимостью хранения как раз и решают данную задачу. Обеспечивая возможность работы с различными периферийными устройствами – накопителями на жестких магнитных дисках, On-Line оптическими стойками, накопителями на магнитной ленте и CD-ROM устройствами. Система обеспечивает **автоматический перенос данных** с на более “дешевые” устройства в случае, если доступ к ним осуществляется недостаточно часто.

Система маршрутизации документов занимается непосредственно пересылкой документов на рабочие места исполнителей, осуществляет сбор информации о текущем статусе документов и консолидацию документов по завершению работы с ними на отдельных этапах, а также обеспечивает средства доступа к информации о текущем состоянии работ с документами.

Системы маршрутизации, как правило, содержат средства описания типовых маршрутов прохождения документов в организации. На основании разработанных маршрутных схем могут порождаться экземпляры бизнес-процессов работы с документами. В данном случае можно говорить о **жесткой маршрутизации**.

Альтернативой является так называемая **свободная маршрутизация**, при которой маршрут формируется “стихийно”. Каждый пользователь системы, обладающий соответствующими правами, может определить следующего или следующих исполнителей документа. Администратор системы и менеджер, курирующий конкретный бизнес-процесс, может контролировать текущее состояние маршрута и вносить различные корректирующие воздействия в случае необходимости.

При маршрутизации документов возможны две схемы, называемые **Off-Line** и **On-Line**.

В первом случае при пересылке документа на рабочее место пользователя происходит его физическое извлечение из архива документов и доставка (например, с помощью электронной почты) на рабочее место клиента. По завершению работы документ обратно погружается в архив. В этом случае система маршрутизации сама является клиентом архива документов и вносит соответствующую информацию в учетную базу данных.

Вторая схема не подразумевает физического перемещение документа. Система маршрутизации документов обеспечивает клиенту интерфейс для доступа к заданиям на обработку документов.

Развитием систем маршрутизации документов являются WorkFlow-системы, или **системы комплексной автоматизации бизнес-процессов**. В отличие от систем маршрутизации документов, **объектом маршрутизации** в них является **совокупность данных** используемых в некотором бизнес-процессе. Пользователь получает на рабочее место информацию о том, что он должен сделать и все необходимые для этого данные. WorkFlow приложение определяет, какое приложение должно быть запущено для реализации функций на данном рабочем месте, и загружает в него необходимые данные. Парадигма WorkFlow системы предполагает, что пользователь должен вы-

полнять только необходимые функции, всю рутинную работу – определение последовательности действий, доставку необходимой информации, контроль своевременности исполнения работы и прочее выполняет система WorkFlow.

Функции WorkFlow приложений выходит за рамки функций систем документооборота, однако, технологии, используемые в данных приложениях очень близки технологиям, используемым в системах маршрутизации документов, к тому же маршрутизация документов может рассматриваться как частный случай задачи построения WorkFlow систем, поэтому мы уделили им некоторое внимание.

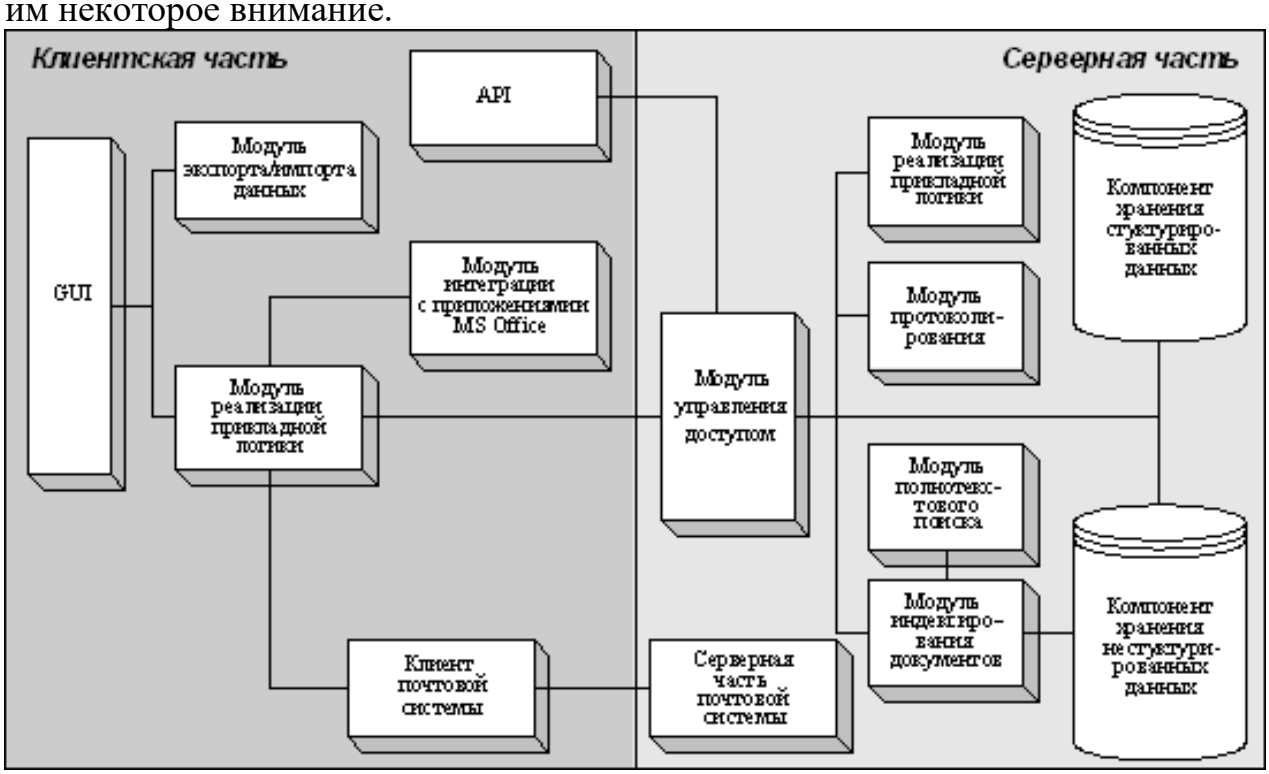


Рисунок 1. Наглядное представление клиентской и серверной части автоматизированного документооборота.

Дополнительно:

Задачи, решаемые системой маршрутизации и контроля исполнения

При организации систем документооборота одной из основных составляющих являются системы маршрутизации и контроля исполнения, которые оперируют документами, хранящимися в архиве. При построении систем маршрутизации могут применяться два основных подхода.

Первый носит название документо-ориентированный. Документ является основным объектом системы, и маршрутизируется именно он, а все остальные параметры маршрутизации ассоциированы именно с документом. Второй подход носит название работо-ориентированный и его основным объектом является работа. К работе может быть прикреплен самый разнообразный список объектов, в том числе, и документы. Естественно, работа может существовать и без документов. Второй подход является более общим.

Свободная маршрутизация

Выделяется два основных типов маршрутов документов. Последовательная маршрутизация - документ последовательно проходит одного исполнителя за другим. Передача документа от одного пользователя к другому может происходить по истечении контрольного времени, либо после завершения работы одним из них. Параллельная маршрутизация - документ одновременно поступает всем исполнителям, а завершение маршрута происходит, когда один либо все пользователи завершат работу с документом.

Системы электронной почты

Минимальной достаточной системой, обеспечивающей маршрутизацию документов, является система электронной почты, которая осуществляет параллельное распространение документов (маршрутизация отличается от распространения или рассылки тем, что маршрутизируемый документ возвращается в начало маршрута, например к инициатору, а рассылаемый документ уходит к исполнителю без контроля факта возврата). С помощью дополнительных приложений система электронной почты может обеспечивать последовательную маршрутизацию документов.

Свободная маршрутизация документов с контролем исполнения

Под контролем исполнения понимается следующая функциональность.

· Контроль доставки задания - инициатору выдается информация о том, что его задание достигло места назначения (исполнителя).

· Контроль прочтения задания - инициатору выдается информация о том, что с его заданием ознакомились сотрудники, для которых это задание было предназначено.

· Контроль выполнения - инициатору выдается информация о том, что задание выполнено.

· Мониторинг задания - инициатор всегда может посмотреть, кто и что сейчас делает с его заданием.

· Извещение о нарушении сроков исполнения - система документооборота может известить инициатора о том, что посланное им задание просрочено конкретным сотрудником.

· История выполнения заданий.

Контроль качества исполнения означает, что, если пользователь говорит о том, что задание исполнено, это еще не означает, что оно действительно исполнено, инициатор должен проверить качество исполнения, подтвердить или нет исполнение.

Информация может выдаваться в виде изменения статуса задания в окнах входящих и исходящих заданий или в виде нового задания, сформированного системой инициатору либо с помощью сообщения по электронной почте.

Маршрутизация документов по заранее определенным маршрутам с контролем исполнения (жесткая маршрутизация)

Маршруты могут быть более сложными, чем простые последовательные или параллельные:

· комбинированные из последовательных и параллельных элементов;

· условные, с переходами в зависимости от состояния тех или иных переменных маршрутов.

Такие маршруты становятся сложными для их задания "на лету", поэтому в этом случае используется специализированный графический редактор, позволяющий создать маршрут. Инициатор вызывает созданный и именованный маршрут и прикрепляет к нему документы - инициирует его. Система маршрутизации должна быть интегрирована с архивной системой, и реальные приложения для работы с документами не могут быть основаны только на файловой системе. И вот почему. Любой процесс маршрутизации документов - это движение одного документа, а не множества его копий, как это происходит в системах электронной почты. Посылать один документ необходимо не только по соображениям экономии пространства, но и в основном для поддержания его целостности - в процессе маршрутизации многие пользователи пытаются вносить изменения в документ. Кроме этого, было бы желательно, чтобы система маршрутизации была интегрирована с архивной системой по следующим параметрам:

· По списку пользователей и системе безопасности. Это означает, что если вы собираетесь послать кому-то документ, то адресат должен обладать соответствующим набором прав для работы с этим документом. Если прав недостаточно, то система должна попросить инициатора работы или маршрута установить соответствующие права.

· Интеграция с операцией публикования документа. Задача состоит в том, что после окончания маршрута документ, ассоциированный с маршрутом, меняет свой статус на опубликованный. В качестве примеров таких маршрутов можно привести процесс утверждения документа.

Рассмотренные возможности обеспечивают построение любой частной системы документооборота на любом предприятии в любой предметной области. Естественно, для построения частного решения можно ограничивать функционал системы в зависимости от предъявляемых заказчиком требований.

Приложение 1
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ДОКУМЕНТООБОРОТА

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль: Менеджмент информационной безопасности
Уровень высшего образования: магистратура
Форма обучения: очная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	Тема:1 -,4	ОПК-1.3. Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении.	ОПК-1.2. Проектирует системы и подсистемы ИБ с учетом современных безопасных инструментальных технологий.	ОПК-1.1. Формирует актуальные модели угроз и нарушителей для современных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности.
2.	ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Тема:1-4	ОПК-3.3. Применяет отечественные стандарты при сертификации средств защиты и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки организационно-распорядительных документов.	ОПК-3.2. Разрабатывает технические задания на создание подсистем обеспечения информационной безопасности.	ОПК-3.1. Исследует и проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	*Инструменты, оценивающие сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ОПК-1 ОПК-3	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-1 ОПК-3	**Тест**	**А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов** **Б) частично сформирована:** • **компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;** • **компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;**	**Например:** **Проводится письменно.** **Время, отведенное на процедуру - 30 минут.** **Неявка – 0 баллов.** **Критерии оценки определяются процентным соотношением.** **Неудовлетворительно – менее 50% правильных ответов.** **Удовлетворительно - от 51% правильных ответов.** **Хорошо - от 70%.** **Отлично – от 90%.** **Максимальная оценка – 5 баллов.**

		В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов	
ОПК-1 ОПК-3	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-1 ОПК-3	***Лабораторная работа***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***1. Оформление в соответствии с требованиями (1 балл).*** ***2. Выбор методов измерений и вычислений (1 балл).*** ***3. Умение применять выбранные методы (1 балл).*** ***4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла).*** ***Максимальная оценка – 5 баллов.***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Исследование выбранного объекта защиты информации – локальной вычислительной сети.

а. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.

2. Разработка требований к системе защиты информации локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

3. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.

4. Разработка пояснительной записки по созданию системы защиты информации выбранного объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

5. Обосновать создание ЛВС, имеющий выход в сеть Интернет. Осуществить выбор средств и организационно – технических мер по защите информации выбранного объекта защиты (с учетом защиты информации от несанкционированного доступа к СЭД).

6. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

7. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД.

8. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД.

9. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

10. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД.

11. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.

12. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию.

13. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД.

14. Разработка проекта подсистемы компьютерной безопасности структурного подразделения предприятия, с учетом применения систем и средств защиты информации от несанкционированного доступа (для СЭД).

Примерная тематика заданий на контрольную работу:

1. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения.
2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения.
3. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS.
4. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 для СЭД.
5. Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП в СЭД предприятия.
6. Задачи и методы добавочных механизмов в рамках усиления парольной защиты в СЭД.
7. Реализация моделей доступа механизмами добавочной и встроенной защиты для СЭД.
8. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия.
9. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия.

10. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.
11. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет.
12. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.
13. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.
14. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.
15. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.
16. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД).
17. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в СЭД.
18. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
19. Информационная безопасность при составление и направление ЭД участником – отправителем.
20. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
21. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Защищенный электронный документооборот» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ОПК-1 ОПК-3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ОПК-1 ОПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Проводится в сроки, установленные	Экзамен	ОПК-1 ОПК-3	3 вопроса	Экзамен т проводится в письменной форме, путем ответа на вопросы.	Результаты предоставляются в день проведения зачета	Критерии оценки: «**Отлично**»: 1. знание основных понятий

графиком образовательного процесса				Время, отведенное на процедуру – 30 минут.		предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание

						неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; **«Неудовле-твори-тельно»**: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

Примерные тестовые задания (форма тестов)
для промежуточного контроля знаний:

1. Что понимается под идентификацией:
процедура распознавания субъекта;
процедура проверки подлинности субъекта;
процедура предоставления субъекту прав доступа;
процесс управления доступом субъектов к ресурсам системы.

2. Сколько компонентов включает в себя система аутентификации:
3;
4;
5;
6.

3. Что понимается под администрированием:
процедура распознавания субъекта;
процедура проверки подлинности субъекта;
процедура предоставления субъекту прав доступа;
процесс управления доступом субъектов к ресурсам системы.

4. Что понимается под аудитом:
процедура распознавания субъекта;
процедура проверки подлинности субъекта;
процесс контроля доступа субъектов к ресурсам системы;
процесс управления доступом субъектов к ресурсам системы.

5. Что понимается под авторизацией:
процедура распознавания субъекта;
процедура предоставления субъекту прав доступа;
процесс контроля доступа субъектов к ресурсам системы;
процедура проверки подлинности субъекта.

6. Назовите основное свойство однонаправленной хэш-функции:
невозможность восстановления исходного значения;
возможность восстановления исходного значения;
возможность редактирования исходного значения;
все значения ключей хэш-функций равны друг другу.

4.2. Типовые вопросы, выносимые на экзамен

1.Назовите процедуры, выполняемые при регистрации пользователя в системе.

2. Что такое аутентификация.

3. Что такое идентификация.

4. Что такое авторизация.

5. Структура модели OSI.

6. Что такое администрирование.

7. Перечислите элементы аутентификации.

8. Для чего служит механизм управления доступом.

9. Перечислите факторы аутентификации.

10. Приведите примеры факторов аутентификации.

11. Назовите методы парольной аутентификации.

12. Приведите пример аутентификации пользователя на основе открытого пароля.

13. Что такое однонаправленные хэш – функции.

14. Что такое PIN- код.

15. назовите области и условие использования PIN- кода.

16. Для чего необходимы парольные политики.

17. Приведите примеры атак на системы, в которых используется аутентификация на основе пароля.

18. Перечислите физиологические биометрические характеристики.

19. Назовите поведенческие биометрические характеристики.

20. Опишите принцип работы биометрических систем.

21. Приведите примеры атак на системы, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от подобных атак.

22. Что такое одноразовые пароли.

23. Опишите принцип работы OTP – токеном метода «запрос – ответ».

24. Приведите пример аутентификации пользователя при использовании OTP – токеном метода «только ответ».

25. Приведите пример аутентификации пользователя при использовании OTP – токеном метода « синхронизация по времени».

26. Приведите пример аутентификации пользователя при использовании OTP – токеном метода « синхронизация по событию».

27. Из каких элементов состоит ключевая пара и для чего предназначен каждый элемент.

28. Что такое ЭЦП? Приведите примеры использования.

29. В каких случаях можно использовать криптографию с открытым ключом.

30. Приведите пример использования криптографии с открытым ключом для шифрования сообщения.

31. Приведите пример аутентификации пользователя с помощью открытых ключей (PKI)..

32. Назовите способы хранения закрытого ключа.

33. Назовите недостатки аутентификации с помощью открытых ключей.

34. Приведите примеры атак на системы, использующие аутентификацию с помощью открытых ключей, и способы защиты от подобных атак.

35. Назовите основные особенности протоколов LAN Manager и NT LAN Manager.

36. Назовите типы аутентификации в NTLM.

37. Приведите примеры атак на системы, использующие аутентификацию с помощью протоколов LANMAN и NTLM, и защиты от них.

38. Перечислите преимущества протокола Kerberos.

39. Опишите функции сервера аутентификации, входящего в состав центра распределения ключей протокола Kerberos.

40. Приведите примеры атак на Kerberos и способы защиты от них.

41. Перечислите преимущества реализации протокола Kerberos в ОС Windows 2000 и последующих ОС в сравнении с более ранними продуктами семейства Windows.

42. Приведите пример способа интеграции шифрования в протокол Kerberos.

43. Возможные атаки на Kerberos + PKINIT и методы защиты от них.

44. Какие протоколы включены в механизм аутентификации Point-to-Point Protocol (PPP).

45. Перечислите основные элементы стандарта 802.1x.

46. Какие методы EAP стандарта 802.1x включены в стандартную комплектацию Windows XP.

47. Опишите взаимодействие между пользователем, клиентом и сервером RADIUS.

48. Опишите метод получения ключей шифрования, используемых для PPP.

49. Какие возможности обеспечивает протокол SSL для безопасности связи.

50. Что включает в себя ассоциация безопасности.

51. Перечислите способы аутентификации при использовании протокола IPSec.

52. Какие протоколы IPSec защитить не может.

53. Преимущества протокола IPSec.

54. На каких этапах должна быть обеспечена безопасность закрытого ключа пользователя.

55. Перечислите подходы к обеспечению безопасности закрытых ключей.

56. Перечислите функции централизованной системы управления.

57. Перечислите основные критерии выбора персонального средства аутентификации и хранения ключевой информации.

Приложение 2
Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ДОКУМЕНТООБОРОТА

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

- формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации в СЭДО;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации в СЭДО, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

Задачи дисциплины:

Научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации и формированием у обучающихся системы знаний, умений и навыков по защите информации, обеспечению информационной безопасности граждан, общества и государства. В том числе:

- построение разрешительной системы доступа к конфиденциальной информации;
- определение номенклатуры дел, формирование и оформление конфиденциальных дел;
- разносторонний обзор систем электронного документооборота;
- раскрытие общих положений по защите информации в СЭД;
- научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации с СЭД;
- ознакомить студентов при решении поставленных задач с помощью перспективных технологий и методов защиты информации;
- ознакомить студентов с методикой применения и использования встроенных механизмов защиты информации;
- ознакомить студентов с порядком применения средств добавочной защиты информации.

2. Указания по проведению практических занятий

3.

Тема 1. Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации. Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации

Практическое занятие 1.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. разрешительная система доступа к документам.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основные сервисы для обеспечения надежной аутентификации и управления доступом
2. Авторизация при доступе к объекту.
3. Система аудита Active Directoru.
4. Назначение и решаемые задачи инфраструктуры открытых ключей.
5. Управление идентификацией (ILM).
6. Microsoft Identity Integration Server (MIIS).
7. Системы обеспечения.

Продолжительность практического занятия-2 часа

Тема 2. Составление номенклатуры дел, формирование и оформление конфиденциальных дел. Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации

Практическое занятие 2.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *практическая работа в группах*.

Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. составление номенклатуры дел и подготовка их для архивного хранения.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Управление доступом в СУБД Oracle с помощью встроенных механизмов безопасности.
2. Управление доступом в СУБД Oracle с помощью криптографических средств защиты.

Продолжительность практического занятия-2 часа

Тема 3: Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации

Практическое занятие 3.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Описание продуктов компании CITRIX SYSTEMS.

2. Компоненты систем, построенных с использованием XenApp.
Продолжительность практического занятия-2 часа

Тема 4: Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота

Практическое занятие 4.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Часть 1: Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003

Часть 2: Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП

Часть 3: Технология программно-аппаратной защиты

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии при построении СЭД.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Часть1:

1.Общие сведения об аутентификации пользователей в домене Windows Server 2003 с помощью цифровых сертификатов и ключей eToken.

2. Установка и настройка Центра сертификации (CA), подготовка консоли Центра сертификации, издание сертификатов

3. Использование ключей eToken для регистрации в домене, для запуска приложений от имени другого пользователя и для подключения сетевых дисков с использованием прав доступа другого пользователя.

Часть2:

1. Общие сведения о безопасном доступе к информационным ресурсам организации.
2. Удаленный доступ к рабочему столу (RDP).
3. Виртуальные частные сети (VPN).
4. Общие сведения о протоколе EAP.
5. Защищенное подключение к Web – серверу (HTTPS).
6. Шифрование и использование ЭЦП.

Часть3:

1. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.

2. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.

3. Механизм удаленного (сетевого) мониторинга активности системы защиты, как альтернатива применению аппаратной компоненте защиты.

Продолжительность практического занятия-2 часа

Тема 5. Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа.

Применение аппаратных средств аутентификации и хранения ключевой информации

Практическое занятие 5.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Часть 1: Метод контроля вскрытия аппаратуры

Часть 2: Электронная цифровая подпись

Цель занятия: ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП).

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.
2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Общий подход к контролю вскрытия аппаратуры техническими средствами защиты.

2. Реализация системы контроля вскрытия аппаратуры.

3. Принципы комплексирования средств защиты информации.

4.Комплексирование механизмов защиты информации от НСД.

5.Комплексирование в одной системе механизмов технической и объектовой защиты информации с единым сервером безопасности.

Продолжительность практического занятия-4 часа

3.Указания по проведению лабораторного практикума.

Цель и задачи выполнения лабораторных работ: Определение порядка и последовательности действий по обоснованию предложений руководителю по результатам анализа и прогноза по заданной ситуации.

Методика *определяется моделью соответствующей задачи, решаемой обучающимся на занятии по заданию преподавателя)* и средства *для* выполнения лабораторных работ: общее *программное обеспечение*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним *(тематика лабораторных работ должна соответствовать рабочей программе дисциплины).*

Лабораторная работа № 1.
Тема: Структура информационных ресурсов и администрирование в компьютерных системах
Цель занятия**:** Определение конфигурации информационных ресурсов компьютерных систем. Администрирование в компьютерных системах.
Продолжительность практического занятия-2 часа
Задание.

ЗАДАНИЕ

Тема: Определение ПЭМИ на примере информативного сигнала видеотракта

Цель работы.

Изучение теоретической основы измерений ПЭМИ на примере показателей информативного сигнала видеотракта. Изучение основных аспектов проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

1. Изучить теоретическую часть Задания №3.
2. Выполнить практическую часть Задания №3:

   а) ответить на вопросы для самопроверки;

   б) выполнить практические задания.

3. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Одним из основных и, зачастую, самых мощных источников сигналов ПЭМИ является видеотракт. Конечно сигнал, который нас интересует, это сигнал интерфейса передачи видеосигнала, но все устройства видеотракта, включающие видеоконтроллер, соединительные кабели, KVM коммутаторы (для систем с несколькими устройствами отображения информации) и конечные устройства отображения (мониторы, прокторы, телевизоры) существенно влияют на уровень сигнала и направление его излучения, потому как выступают в качестве антенн.

Приведем список наиболее популярных видео-интерфейсов: аналоговый:

- VGA (несмотря на широкое развитие современных цифровых

интерфейсов имеет широкое распространение и еще долгое время будет эксплуатироваться на большинстве АС);

цифровые:

- DVI (бывает совмещен с VGA и применяются переходники VGADVI, в таком случае рассматривается как VGA);
- HDMI;
- DisplayPort.

Немного забегая вперед, для анализа интерфейса рассмотрим один из способов определения частот сигналов ПЭМИ – непосредственное подключение к линии передачи сигнала, путем использования специального кабеля с выводами для подключения. Рассмотрение будем вести на примере VGA интерфейса в силу простоты сигнала, схожего с телевизионным, а также стабильности и понятности задания тестового режима. Не имеет значения к какому из проводов, передающих цвет (R, G или B) подключаться, так как

при формировании тестового режима, обеспечивающего максимальную частоту следования импульсов, на экран монитора выводится статическая засветка пиксель белый, пиксель черный, пиксель белый и т. д. При формировании белой точки сигнал присутствует в проводе каждого из цветов (рис. 1).

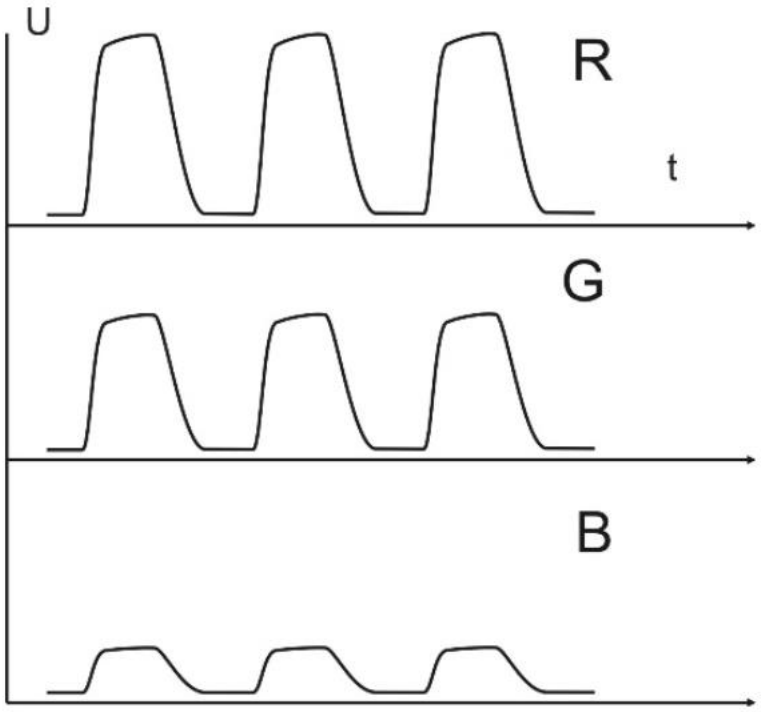
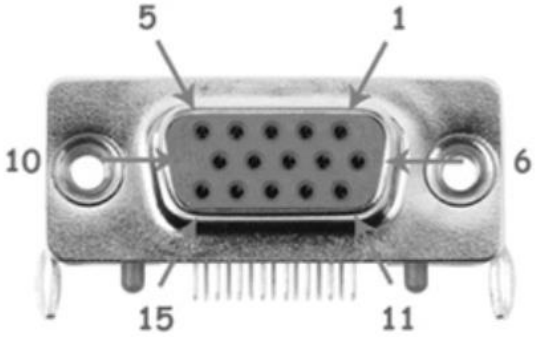


Рисунок 1. Осциллограммы сигналов в RGB интерфейсе

Распиновка разъема VGA информационного кабеля приведена на (рис. 2)



№	Наименование	Описание
1	RED	Красный сигнал
2	GREEN	Зеленый сигнал
3	BLUE	Синий сигнал
4	n/c	Не используется
5	GND	Земля
6	RED_RTN	Красный земля
7	GREEN_RTN	Зеленый земля
8	BLUE_RTN	Синий земля
9	VDC	+5В
10	GND	Земля
11	ID0	Идентификатор монитора
12	SDA	DDC / I2C data
13	HSYNC	Горизонтальная синхронизация
14	VSYNC	Вертикальная синхронизация
15	SCL	DDC / I2C clock

Рисунок 2. Распиновка разъема информационного кабеля VGA интерфейса

Кабель для данного вида исследований изготавливается специально и используется исключительно для определения частот сигналов ПЭМИ VGA интерфейса, измерения необходимо строго производить именно с тем кабелем, с которым будет эксплуатироваться АС. Структура сигнала представляется следующим образом.

С кадровой частотой (например, 60 Гц) следуют «пачки» импульсов, формирующих каждый кадр на экране монитора (рис. 3).

Кадровые «пачки» импульсов состоят в свою очередь из строчных последовательностей импульсов, каждая из которых задает сигнал для формирования строки на экране монитора (частота следования при разрешении 1024 × 768 в 768 чаще, чем кадровая, то есть около 46 кГц, рис. 4).

Строчные «пачки» импульсов состоят уже непосредственно из импульсов с переходами из 0 в 1, соответствующим тестовому режиму (пиксель белый, пиксель черный и т. д.).

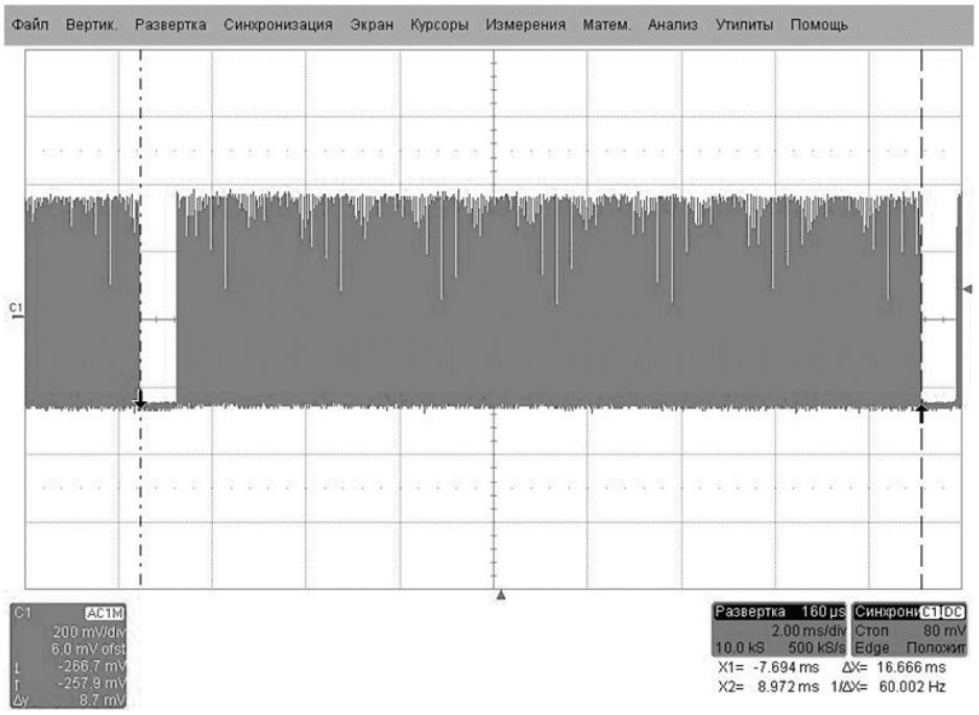


Рисунок 3. Кадровые видеоимпульсы

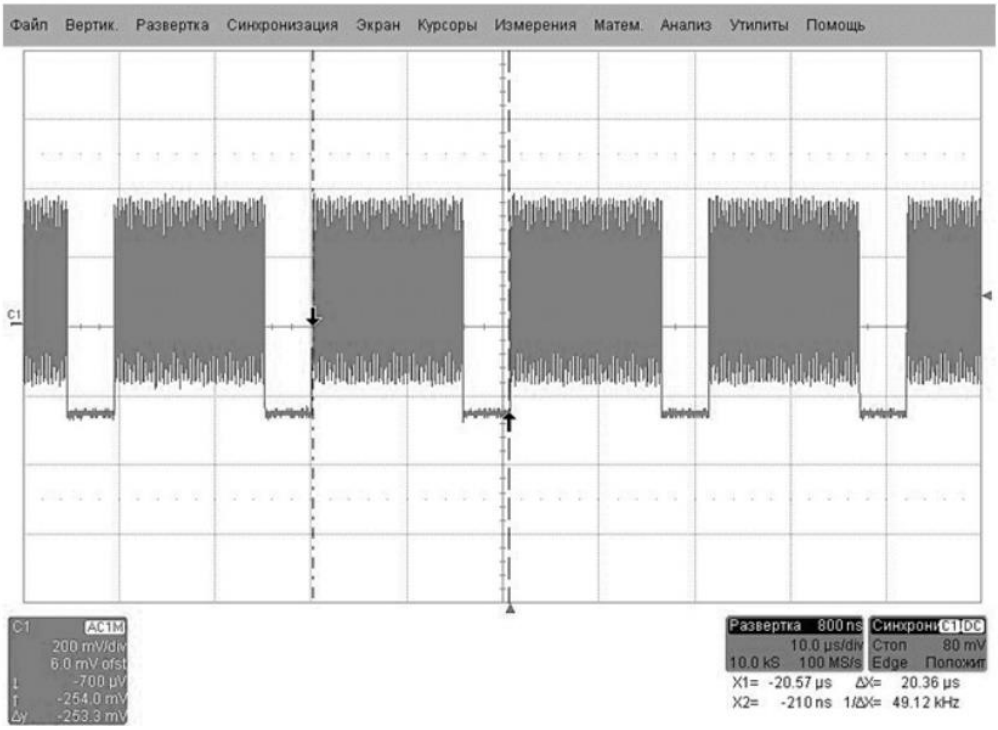


Рисунок 4. «Пачки» строчных видеоимпульсов

В результате, частота следования импульсов, задающих черные и белые пиксели и будет тактовой частотой (частотой первой гармоники) нашего сигнала ПЭМИ от видеотракта (в данном случае 32,5 МГц, можно также для уточнения применять режим БПФ). Следует отметить, что подобные кабели (с отводами для подключения осциллографа) используются только на этапе анализа сигналов, при измерениях необходимо в обязательном порядке применять кабели, с которыми в дальнейшем будет эксплуатироваться данная АС.

Сложнее дело обстоит с цифровыми видео интерфейсами, например, DVI, в основе которого лежит технология TMDS. Суть данной технологии заключается в том, что на каждый цвет приходится по две пары. Воздействие возможных помех будет производиться одинаково на оба провода, а, следовательно, их можно будет легко отфильтровать. Также в интерфейсе применяется технология минимизации количества переходов из «0» в «1» (и наоборот), что также сказывается на помехозащищенности интерфейса.

К сожалению, все это усложняет задачу для формирования тестового сигнала, который, наоборот, должен обеспечивать максимальную частоту следования импульсов в канале. У протокола TMDS есть одна особенность. Если длительное время передается сплошной поток «1», то в силу того, что кабель обладает определенной емкостью, спад уровня с «1» до «0» может произойти с задержкой, следовательно, произойдет потеря пакетов. Для того чтобы этого избежать, в таких ситуациях, протокол TMDS в конце каждых 8 битов добавляет бит DC-Balancing, который указывает на что, что следующие 8 битов будут инвертированы. В результате получаем последовательность импульсов с постоянными и стабильными переходами. Тактовая частота первой гармоники DVI интерфейса при данном тестовом режиме и стандартных разрешениях не выше 1600 × 1280 × 60 Гц лежит в пределах 130...170 МГц.

Интерфейсы HDMI и DisplayPort строятся также с применением технологии TMDS, но с увеличением скорости передачи данных, способ задания

тестового режима остается такой же, только тактовые частоты будут гораздо выше, возможно даже за пределами исследуемого нами диапазона частот.

Практическая часть.

Вопросы для самопроверки:

1) Что такое видеоинтерфейс?
2) Какие интерфейсы есть у информационного кабеля для видео? Перечислите.
3) Чем отличаются кадровые «пачки» импульсов от строчных?
4) Какая частота приемлема для видео с интерфейсом VGA?
5) С каким видеоинтерфейсом больше всего возникает проблем при измерении?

Практические задания:

1) На Ваш взгляд, что нужно сделать при проведении измерений видеосигнала? Опишите начало измерений от получения технического средства для проведения исследований до передачи его обратно в комплект поставки. Для данного задания можете попросить помощи у Вашего преподавателя.
2) Как Вы считаете, что такое меандр информативного сигнала? Опишите это явление на примере информативного сигнала монитора с интерфейсом VGA.

Лабораторная работа № 2.
Тема: Анализ угроз информационной безопасности

Цель занятия: Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.

Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.

Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

Продолжительность практического занятия-2 часа
Задание.
(см. задание л.р.№1)

Лабораторная работа № 3.
Тема: Основные уровни защиты информации в компьютерных системах
Цель занятия: Методы и средства обеспечения защиты информации в компьютерных системах. Защита представления информации. Защита содержания информации.
Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.
Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок. Аппаратные средства защиты в КС. Задачи, решаемые программными средствами защиты.
Продолжительность практического занятия-4 часа
Задание. (см. задание л.р.№4)

Лабораторная работа № 4.
Тема: Основные положения формальной теории защиты информации
Цель занятия: Концепция монитора безопасности обращений в КС.
Правила разграничения доступа субъектов к объектам в ОС.
Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО
Продолжительность практического занятия-4 часа
Задание.

ЗАДАНИЕ

Тема: Средства защиты информации

Цель работы.

Изучение теоретической основы активных средств защиты. Изучение основных аспектов настройки и эксплуатации средств защиты.

Продолжительность занятия: полтора учебных часа.

Задания.

4. Изучить теоретическую часть Задания №4.

5. Выполнить практическую часть Задания №4:
   а) ответить на вопросы для самопроверки;
   б) выполнить практические задания.
6. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Целью защиты информации от утечки по ТКУИ является уменьшение отношения «сигнал/шум». Уменьшение может осуществляться с помощью применения пассивных и/или активных методов и средств защиты.

Активный метод заключается в перекрытии полезного сигнала более мощным шумом. Данный метод защиты осуществляется аппаратное, через специальные устройства так называемые «Генератор шума». Генераторы шумов специально создают мощные электромагнитные излучения, которые не имеют информативной ценности и затрудняют или делают совсем невозможным анализ полезного сигнала относительно окружающего шума. Надо заметить, что генераторы шумов от побочных электромагнитных излучений имеют свои недостатки, такие как:

- довольно мощные источники излучения не являются полезным для здоровья;
- наличие маскирующего сигнала говорит о наличие конфиденциальной информации;
- нельзя гарантировать абсолютную защищенность информации.

Пассивный метод заключается в уменьшении мощности самого излучаемого сигнала. Осуществление подобного метода заключается в изоляции излучающих проводников, устройств, а также периметра помещения специальными материалами поглощающими ЭМП, в отношении проводных линий – установка фильтров.

Активные методы основаны на увеличении уровня шума путем применения генераторов пространственного зашумления. Данные устройства, как

правило, формируют широкополосную помеху во всем диапазоне частот. Регулировка в большинстве моделей осуществляется только по общему уровню сигнала, за редким исключением присутствует возможность корректировки частотной характеристики на низких, средних и высоких частотах.

С точки зрения заключения договора на аттестацию ОИ применение САЗ самый удобный и простой вариант, а иногда и единственный (если организация арендует 1-2 помещения и расстояние до границы КЗ 1 м).

Наиболее популярные модели САЗ по каналу ПЭМИН приведены. приведен скан сертификата ФСТЭК России на САЗ «Соната-Р3.1».

Рисунок 1. Средство активной защиты от утечек за счет ПЭМИН «Соната-Р3.1»

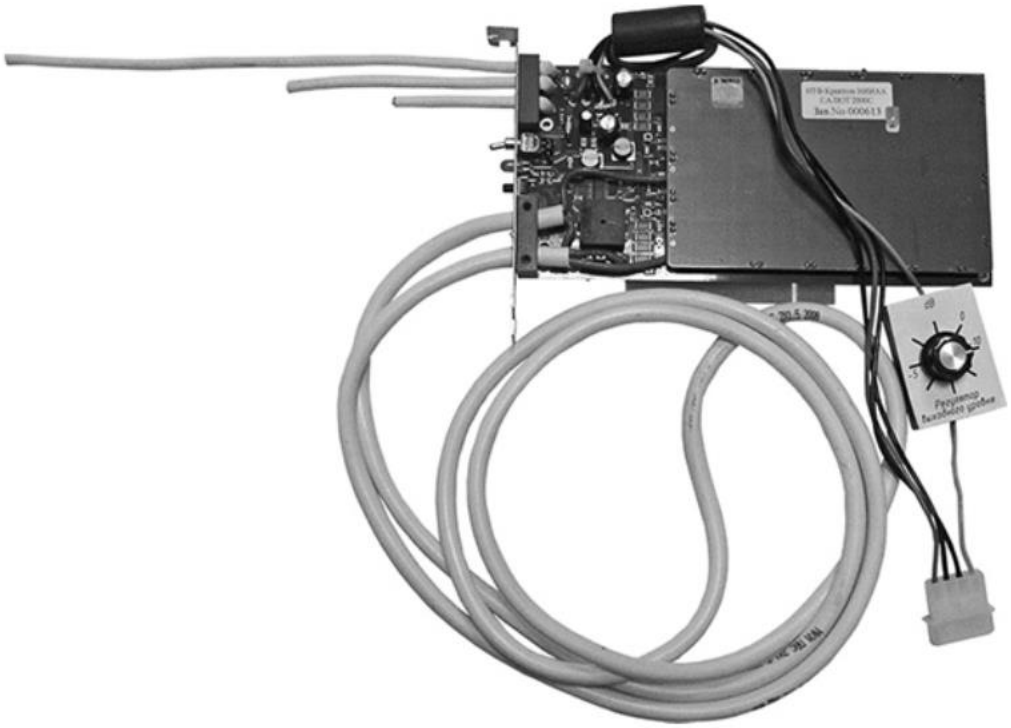
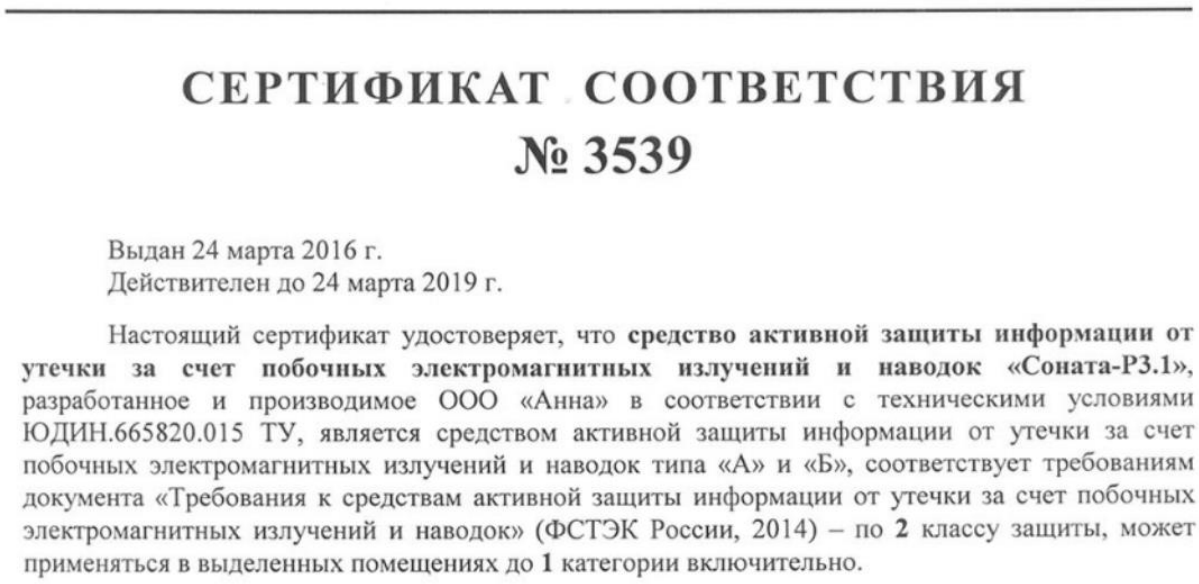


Рисунок 2. Средство активной защиты информации от утечек за счет ПЭМИН «Салют 2000С»



СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3539

Выдан 24 марта 2016 г.
Действителен до 24 марта 2019 г.

Настоящий сертификат удостоверяет, что **средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «Соната-Р3.1»**, разработанное и производимое ООО «Анна» в соответствии с техническими условиями ЮДИН.665820.015 ТУ, является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа «А» и «Б», соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по **2** классу защиты, может применяться в выделенных помещениях до **1** категории включительно.

Рисунок 3. Сертификат соответствия ФСТЭК России на СЗИ «Соната-Р3.1»

Исходя из графика спектров помех можно сделать вывод, что во всем диапазоне частот помехи не обладают равномерным спектром. Вследствие чего, при проведении измерений, сигналы ПЭМИ могут оказаться на частотах, соответствующих «провалам» в спектре помехи, что поставит под вопрос защищенность объекта. Проблема в том, что с точки зрения требований по сертификации САЗ по каналу ПЭМИН, оценивается только спектральная плотность мощности, причем в достаточно широкой полосе, а то, как ведет себя спектр помехи в данной полосе это уже будет видно на практике (для примера приведем характеристики САЗ «Соната-Р2», табл. 2–4).

Таблица 2

Спектральная плотность напряженности электрической составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Вертикальная поляризация, дБ		Горизонтальная поляризация, дБ	
	Без дополнительной антенны	С дополнительной антенной	Без дополнительной антенны	С дополнительной антенной
от 0,01 до 0,15	50	80	50	80
от 0,15 до 1	45	70	40	70
от 1 до 5	45	60	40	55
от 5 до 30	45	60	40	50
от 30 до 100	40	50	40	50
от 100 до 1000	30	30	30	30
от 1000 до 2000	30	30	30	30

Таблица 3

Спектральная плотность напряженности магнитной составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,15	30	30
от 0,15 до 4	35	35
от 4 до 10	40	40
от 10 до 30	30	35

Таблица 4

Спектральная плотность напряжения помех в линиях электропитания и заземления «Соната-Р2», не менее

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,04	25	25
от 0,04 до 10	35	35
от 10 до 100	35	45
от 100 до 600	25	25
от 600 до 1000	15	15

Пассивные методы защиты информации от утечки по каналам ПЭМИН возможно реализовать следующими путями:

- уменьшение уровня информативного сигнала за счет экранирования помещения (что практически невозможно, гарантию может дать только специализированная экран камера, которая применяется для лабораторных исследований источников радиосигналов).
- если в процессе анализа выявлено, что ТКУИ возникает только за счет наводок на линии электропитания, то возможно применение сетевых подавляющих фильтров (рисунок 3).

Рисунок 3. Фильтр сетевой помехоподавляющий ЛФС-10-1Ф

Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц

«ЛФС-10-1Ф» соответствует: типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания.

«ЛФС-10-1Ф» соответствует документу «Требования к пассивным средствам защиты информации от побочных электромагнитных наводок на линии электропитания» (ФСТЭК России, 2015), – по 1 классу защиты.

Отметим, что на практике чаще всего в случае невыполнения норм защищенности применяются средства активной защиты – генераторы электромагнитного шума, которые также создают наведенную помеху на линии и токоведущие коммуникации.

Практическая часть.

Вопросы для самопроверки:

6) Опишите самый простой и удобный способ на аттестацию ОИ при применении САЗ.
7) По какому классу защиты соответствует ЛФС-10-1Ф?
8) Что такое активная защита САЗ?
9) Что такое пассивная защита САЗ?
10) Какими методами по защите информации от утечек ПЭМИН возможно реализовать пассивные меры защиты?

Практические задания:

3) По вашему мнению, является ли допустимым использование одновременно и пассивных и активных мер защиты? Если возможно, в подробности расскажите почему?

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных

защищенных систем ЭДО;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

№ п/п	Наименование блока (раздела) дисциплины	**Виды СРС**
2 семестр		
1	Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации	1. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД. 2. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД. 3. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2	Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации. Составление номенклатуры дел, формирование и оформление конфиденциальных дел	1. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД. 2. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.
3	Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации	1. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	Система защищен-	1. Разработка и обоснование требований к си-

	ного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота.	стеме защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

Вопросы, выносимые на самостоятельное изучение:

1. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения.
2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения.
3. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS.
4. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 для СЭД.
5. Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП в СЭД предприятия.
6. Задачи и методы добавочных механизмов в рамках усиления парольной защиты в СЭД.
7. Реализация моделей доступа механизмами добавочной и встроенной защиты для СЭД.
8. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия.
9. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия.

10. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.

11. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет.

12. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.

13. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

14. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

15. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

16. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД).

17. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в СЭД.

Примерные темы докладов

1. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД.

2. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД.

3. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

4. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию.

7. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД.

8. Разработка проекта подсистемы компьютерной безопасности структурного подразделения предприятия, с учетом применения систем и средств защиты информации от несанкционированного доступа (для СЭД).

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6.. Перечень основной и дополнительной учебной литературы необходимой для освоения дисциплины (модуля)

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3.Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. - Москва : КУРС, 2023. - 296 с. - ISBN 978-5-906923-24-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902497 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
4.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
5.Моргунов, А. В. Электронные системы документооборота : учебное пособие / А. В. Моргунов. - Новосибирск : Изд-во НГТУ, 2020. - 74 с. - ISBN 978-5-7782-4269-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1870515 (дата обращения: 30.11.2022). – Режим доступа: по подписке.

Дополнительная литература:

6.Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
7.Раздорожный, А. А. Документирование управленческой деятельности : учеб. пособие / А.А. Раздорожный. — Москва : ИНФРА-М, 2018. — 304 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011744-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/969585 (дата обращения: 30.11.2022). – Режим доступа: по подписке.
8.Информационные технологии в документационном обеспечении управления и архивном деле : учебник для вузов / Н. Н. Кунаев, Т. В. Кондрашова, Е. В. Терентьева, А. Г. Фабричнов / под общ. ред. Н. Н. Куняева. - Москва : Логос, 2020. - 408 с. - ISBN 978-5-98704-786-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211641 (дата обращения: 30.11.2022). – Режим доступа: по подписке

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.

2. http://informika.ru/ – образовательный портал.

3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн.

5. www.rucont.ru - ЭБС «Руконт».

6. http://www.academy.it.ru/ – академия АЙТИ.

7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации

8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**

9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8.. Перечень информационных технологий, , используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: MSOffice, Multisim.

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант)