МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ КОМПЬЮТЕРНЫХ И ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК

КАФЕДРА ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Отчёт по лабораторной работе № 1 по дисциплине «Методы и средства защиты информации»

**Ознакомление с основными ОРД по ИБ составление реестров документов в разбивке по группам с указанием краткого содержания**

|  |  |
| --- | --- |
| Выполнил: студент группы ФИб-4302-51-00 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Д.А. Савин / |
| Проверил: доцент каф. ПМиИ | \_\_\_\_\_\_\_\_\_\_\_\_\_/ Д.Ю. Ляпунов / |

Киров 2021

**Cодержание**

[Введение 3](#_Toc88041085)

[1 Анализ предметной области 4](#_Toc88041086)

[1.1 Основные понятия и определения 4](#_Toc88041087)

[2 Организационно-распорядительная документация 6](#_Toc88041088)

[Заключение 14](#_Toc88041089)

[Библиографический список 15](#_Toc88041090)

Приложение Отчет по лабораторной работе 1.docx, 55 КБ, редакция от 4.11.2021, Отправлен в Teams 8.11.2021 Ляпунову Д.Ю.

# Введение

**Цель работы:** научиться составлять реестры с организационно-распорядительными документами по информационной безопасности.

**Задачи:**

1. Поиск источников информации по данной теме.
2. Составление реестра с ОРД по ИБ в разбивке по группам.
3. Формулировка соответствующих выводов.
4. Разработка тестов для закрепления материала.

# Анализ предметной области

## Основные понятия и определения

Организационно-распорядительная документация (ОРД) — комплекс документов, закрепляющих функции, задачи, цели, а также права и обязанности работников и руководителей по выполнению конкретных действий, необходимость которых возникает в операционной деятельности организации. Информация — сведения (сообщения, данные) независимо от формы их представления. Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. В соответствии с ГОСТ 33707–2016 (ISO/IEC 2382:2015) [5, c.16]

Информационные технологии. Словарь, информационная система — это система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию. Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Также к правовым понятиям следует отнести понятие прав доступа к защищаемой информации. [5, c.17]

Ограничения доступа устанавливаются к сведениям, составляющим государственную тайну и иные виды тайны. В качестве собственников информации рассматриваются государство, организации и граждане (юридические и физические лица). Доступ к информации — возможность получения информации и ее использования. Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц. Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. Утечки информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной.

# 2 Организационно-распорядительная документация

|  |  |  |
| --- | --- | --- |
| 1.Указы Президента | | |
| Название | Дата | Краткое содержание |
| 1.№ 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”Указ Президента Российской Федерации от 05.12.2016 г. № 646Указ Президента Российской Федерации от 05.12.2016 г. № 646 | 05.12.2016 (срок действия не обозначен) | Система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. |
| 2.№ 188 "Об утверждении перечня сведений конфиденциального характера" | 06.03.1997 (ред. от 13.07.2015) | Утверждается перечень сведений конфиденциального характера |
| 3.№ 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне" | 30.11.1995 (ред. от 25.03.2021) | Утверждается перечень сведений, отнесенных к государственной тайне |
| 4.№ 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела" | 30.05.2005 (ред. от 11.03.2021) | Определяется порядок обработки персональных данных государственного гражданского служащего Российской Федерации |
| 2.Постановления Правительства | | |
| 5.№ 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" | 01.11.2012 (действующий) | Документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных. |
| 6.№ 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" | 21.03.2012(ред. от 15.04.2019) | Утверждение перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" |
| 7.№ 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" | 15.09.2008 | Утверждение положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации |
| 3.Федеральные законы | | |
| 8.№ 149-ФЗ "Об информации, информационных технологиях и о защите информации" | 27.07.2006 (ред. от 01.10.2021) | Описание понятий и определений в области технологии правового регулирования в сфере информации, информационных технологий, а также регулирование отношений при осуществлении права на поиск, получение, передачу, производство и распространение информации при применении информационных технологий |
| 9.№ 187-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях" | 02.07.2013 (ред. от 12.03.2014) | Закон подразумевает возможность блокировки сайтов, содержащих нелицензионный контент, по требованию правообладателя. |
| 10.№152-ФЗ О персональных данных | 27.07.2006 | О регулировании отношений, связанных с обработкой персональных данных, осуществляемой федеральными органами государственной власти и др. |
| 4.Стандарты ГОСТ | | |
| 11.ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования | 01.01.1996 | Настоящий стандарт устанавливает единые функциональные требования к защите средств вычислительной техники от несанкционированного доступа к информации |
| 12.ГОСТ Р 50922-2006 Защита информации. Основные термины и определения | 01.02.2008 | Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации. |
| 13.ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство | 01.07.1999 | Настоящий стандарт распространяется на испытания программных средств и их компонентов, цели которых - обнаружить в этих программных средствах и устранить из них компьютерные вирусы силами специальных предприятий |
| 5. Документы уполномоченных федеральных органов | | |
| 14.Приказ ФСБ России от № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических средств защиты информации (Положение ПКЗ-2005))» | 03.03.2005  (ред. от 12.04.2010) | Утверждение прилагаемого положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) |
| 15.Приказ ФСБ России № 416 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» | 31.08.2010 | Утверждение прилагаемых требований о защите информации, содержащейся в информационных системах общего пользования. |
| 16.Приказ ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» | 18.02.2013 | Утверждение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. |
| 6.Должностные инструкции из Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации" | | |
| 17.Главный специалист по технической защите информации |  | Руководит выполнением работ по технической защите информации в организациях. Организует проведение категорирования объектов информатизации, выявление угроз безопасности информации |
| 18.Начальник отдела (лаборатории, сектора) по противодействию техническим разведкам |  | Выполняет работы по противодействию техническим разведкам в организациях оборонно-промышленного комплекса. Руководит работами по выявлению каналов утечки информации |
| 19.Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры |  | Выполняет мероприятия по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Определяет возможные угрозы безопасности информации, уязвимость программного и аппаратного обеспечения |
| 7.Руководящие документы | | |
| 20.Разработан в дополнение к РД 50-680-88 Автоматизированные системы. Защита от несанкционированного  доступа к информации. Классификация автоматизированных систем  и требования по защите информации | 30.03.1992 | Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. |
| 21.№114. Защита от несанкционированного доступа к информации. | 04.06.1999 | Настоящий руководящий документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. |
| 22.Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. | 30.03.1992 | Настоящий документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД). |
| 23.Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации | 30.03.1992 | Устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований. |
|  | 8.Стандарты ISO |  |
| 24.ISO/IEC 27000:2018 Information security management systems - Overview and vocabulary (Система менеджмента информационной безопасности. Общий обзор и терминология) | 02.2018 | Содержит обзор систем управления информационной безопасностью (СУИБ). В нем также содержатся термины и определения, обычно используемые в семействе стандартов СУИБ. |
| 25.ISO/IEC 27001:2005, Information security management systems - Requirements (Система менеджмента информационной безопасности. Требования) | 10.2013 | Определяет требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы управления информационной безопасностью в контексте организации. |
| 26.ISO/IEC 27002:2013, Code of practice for information security management (Свод правил по управлению защитой информации) | 10.2013 | Содержит рекомендации по стандартам информационной безопасности организации и методам управления информационной безопасностью, включая выбор, внедрение и управление средствами контроля с учетом среды (сред) рисков информационной безопасности организации. |

Тестовые вопросы

Савин Д.А, Ознакомление с основными ОРД по ИБ составление реестров документов в разбивке по группам с указанием краткого содержания, 6.11.2021

1. **Документ, адресованный вышестоящему руководителю, с изложением конкретной проблемы или постановкой вопроса и содержащий ответы и предложения:**
   1. Объяснительная записка;
   2. Докладная записка;
   3. Информационное письмо;
   4. Письмо-извещение.
2. **Локальный организационно-правовой документ, устанавливающий для работника организации (подразделения) конкретные трудовые (должностные) обязанности в соответствии с занимаемой должностью:**
3. Должностная инструкция;
4. Приказ руководителя;
5. Штатное расписание;
6. Устав организации.
7. **Письмо, своевременно информирующее заинтересованное должностное лицо или организацию о свершившимся факте:**
8. Акт;
9. Докладная записка;
10. Информационное письмо**;**
11. Справка.
12. **Документ, объясняющий вышестоящему непосредственному руководителю причины невыполнения какого-либо поручения, нарушения трудовой или технологической дисциплины:**
13. Докладная записка;
14. Объяснительная записка;
15. Акт о нарушении трудовой дисциплины;

|  |  |
| --- | --- |
| Вопрос | Ответ |
| 1 | 2 |
| 2 | 1 |
| 3 | 3 |
| 4 | 2 |
| 5 | 3 |

1. Письмо-извещение.

**5. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

1. Актуальность;
2. Доступность;
3. Целостность.
4. Конфиденциальность.

# Заключение

В ходе лабораторной работы были выделены основные группы организационно-распорядительных документов по информационной безопасности, проведен анализ этих документов и составлен реестр документов с разбивкой на группы.

# Библиографический список

1. Консультант Плюс [Электронный ресурс] – 1997 URL: <http://www.consultant.ru/> (дата обращения: 29.09.2021)
2. Сайт Президента России [Электронный ресурс] – 2021 URL: <http://www.kremlin.ru/acts/bank> (дата обращения: 29.09.2021)
3. Информационно-правовой портал Гарант.ру [Электронный ресурс] – URL: <https://www.garant.ru/doc/law/> (дата обращения: 29.09.2021)
4. Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] – URL: <https://www.rst.gov.ru/portal/gost> (дата обращения: 29.09.2021)