

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОГО ЗАДАНИЯ №2**

**В РАМКАХ ДИСЦИПЛИНЫ «ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

**Цель:** провести анализ действующих терминов и определений в сфере защиты информации, а также документов их определяющих, научиться использовать систему понятий в области информационной безопасности в профессиональной деятельности.

Диаграмма родовых отношений на основании текста ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» отображена на рисунке 1.

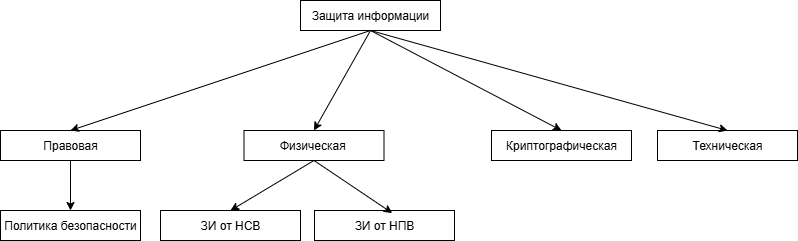


Рисунок 1 - Родовые отношения

Термины используемые в диаграмме

**Защита информации;**ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

**Правовая защита информации:** Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

**Техническая защита информации:** ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

**Криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования.

**Физическая защита информации:** Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

**Защита информации от несанкционированного воздействия:**ЗИ от НСВ: Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**Защита информации от непреднамеренного воздействия:**Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**Политика безопасности (информации в организации):**Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Ресурс - https://meganorm.ru/Data2/1/4293836/4293836037.htm

Диаграмма партитивных отношения на основании ГОСТ 53114-2008 представлена на рисунке 2.

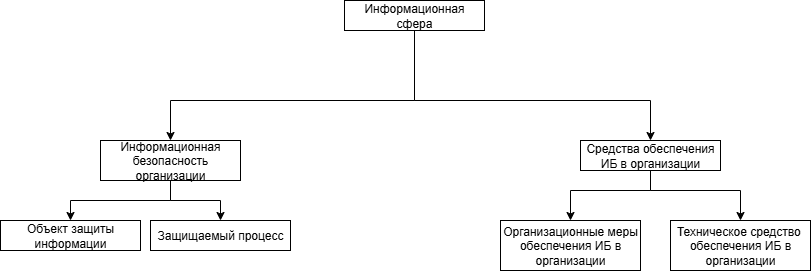


Рисунок 2 - Партитивные отношения

Термины используемы в диаграмме.

**Информационная сфера:** Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

**Информационная безопасность организации:** **ИБ организации;** Состояние защищенности интересов организации в условиях угроз в информационной сфере.

**Объект защиты информации:** Информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.

**Защищаемый процесс (информационной технологии):** Процесс, используемый в информационной технологии для обработки защищаемой информации.

**Обеспечение информационной безопасности организации**: обеспечение ИБ организации: Деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

**Организационные меры обеспечения информационной безопасности:** организационные меры обеспечения ИБ: Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

**Техническое средство обеспечения информационной безопасности:** техническое средство обеспечения ИБ: Оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами.

Ресурс - https://meganorm.ru/Data/484/48411.pdf