**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования**

**«Юго-Западный государственный университет»**

**Кафедра ЗИиСС**

**Практическая работа №1**

**на тему: «Определение класса государственной информационной системы (ГИС)».**

**Ст. преподаватель к.т.н., Волокитина Е.С.**

**2014 г.**

**Оглавление**

[**Цель работы: 3**](#_Toc397339748)

[**1. Требования к выполнению задания: 3**](#_Toc397339749)

[**2. Задание: 3**](#_Toc397339750)

[**3. Теория 4**](#_Toc397339751)

[**4. Ход работы: 8**](#_Toc397339752)

[**5. Вопросы 9**](#_Toc397339753)

[**Список дополнительной литературы: 9**](#_Toc397339754)

**Цель работы:**

определение класса государственной информационной системы (ГИС).

1. **Требования к выполнению задания:**

Ознакомиться и изучить основные принципы разработки организационно-правовых аспектов деятельности службы защиты информации.

1. **Задание:**

Выбрать самостоятельно организацию и информационную систему в ней сделать описание системы и провести ее классификацию.

1. **Ход работы:**

1. **Определение уровня защищенности персональных данных.**

Текст классификации формируется строго с формулировками из ПП №1199.

Тип угроз:

* определяется в Модели угроз (пункт 5.2) и дублируется в Акте определения возможностей.

Итоговый уровень защищенности персональных данных определяется по следующей схеме:

| **НЕ работники** | **угрозы 1 типа** | **угрозы 2 типа** | **угрозы 3 типа** | **Работники** |
| --- | --- | --- | --- | --- |
| **Угрозы с НДВ ОС** | **Угрозы с НДВ СПО** | **Угрозы БЕЗ НДВ** |
| специальные категории | **1УЗПДн** |  |  | специальные категории |
| специальные категории персональных данных **более** чем 100000 |  | **1УЗПДн** |  |  |
| специальные категории персональных данных **менее** чем 100000 |  | **2УЗПДн** |  | специальные категории |
| специальные категории персональных данных **более** чем 100000 |  |  | **2УЗПДн** |  |
| специальные категории персональных данных **менее** чем 100000 |  |  | **3УЗПДн** | специальные категории |
| биометрические | **1УЗПДн** |  |  | биометрические |
| биометрические |  | **2УЗПДн** |  | биометрические |
| биометрические |  |  | **3УЗПДн** | биометрические |
| иные категории | **1УЗПДн** |  |  | иные категории |
| иные категории персональных данных **более** чем 100000 |  | **2УЗПДн** |  |  |
| иные категории персональных данных **менее** чем 100000 |  | **3УЗПДн** |  | иные категории |
| иные категории персональных данных **более** чем 100000 |  |  | **3УЗПДн** |  |
| иные категории персональных данных **менее** чем 100000 |  |  | **4УЗПДн** | иные категории |
| общедоступные | **2УЗПДн** |  |  | общедоступные |
| общедоступные персональные данные **более** чем 100000 |  | **2УЗПДн** |  |  |
| общедоступные персональные данные **менее** чем 100000 |  | **3УЗПДн** |  | общедоступные |
| общедоступные |  |  | **4УЗПДн** | общедоступные |

**2. Определение класса защищенности**

п.1.1. – в большинстве случаев будет персональные данные (но могут быть несколько видов информации, по количеству видов информации ограниченного доступа)

п.1.2. – расставляется по 1 плюсу в каждом столбце в нужной строке, в соответствии с экспертной оценкой для конкретной системы. Соответствие:

|  |  |
| --- | --- |
| **существенные**  негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности  и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять **возложенные на них функции** | **Высокая** |
| **умеренные**  негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности  и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять **хотя бы одну из возложенных на них функций** | **Средняя** |
| **незначительные**  негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности  и (или) оператор (обладатель информации) могут выполнять возложенные на них функции **с недостаточной эффективностью** или выполнение функций возможно только **с привлечением дополнительных сил и средств** | **Низкая** |

п.1.3. – оценка общего УЗ (уровня значимости информации) – он устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации. Соответствие:

|  |  |
| --- | --- |
| хотя бы для **одного**  из свойств безопасности информации (конфиденциальности, целостности, доступности) определена **высокая степень ущерба** | УЗ 1 |
| хотя бы для **одного**  из свойств безопасности информации (конфиденциальности, целостности, доступности) определена **средняя степень ущерба**  и нет ни одного свойства, для которого определена высокая степень ущерба | УЗ 2 |
| для **всех** свойств безопасности информации (конфиденциальности, целостности, доступности) определены **низкие степени ущерба** | УЗ 3 |
| обладателем информации (заказчиком) и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) **не может быть определена**, но при этом информация **подлежит защите** в соответствии с законодательством Российской Федерации | УЗ 4 |

При обработке в ИС двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) УЗ определятся отдельно для каждого вида информации.

п.1.4. – оценка масштаба системы из трёх возможных. Варианты:

|  |  |
| --- | --- |
| Информационная система имеет: | **Если она:** |
| **федеральный масштаб** | функционирует на территории Российской Федерации (в пределах федерального округа) **и**  имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях |
| **региональный  масштаб** | функционирует на территории субъекта Российской Федерации и имеет сегменты **в одном или нескольких**  муниципальных образованиях **и (или)** подведомственных и **иных**  организациях |
| **объектовый масштаб** | функционирует **на объектах одного**  федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации **и не имеет** сегментов в территориальных органах, представительствах, филиалах, подведомственных и **иных** организациях |

п. 1.5. – присвоение класса защищенности информационной системы по табличке сопоставления УЗ и масштаба. Соответствие:

|  |  |  |  |
| --- | --- | --- | --- |
| **Уровень значимости информации** | **Масштаб информационной системы** | | |
| **Федеральный** | **Региональный** | **Объектовый** |
| УЗ 1 | **К1** | **К1** | **К1** |
| УЗ 2 | **К1** | **К2** | **К2** |
| УЗ 3 | **К2** | **К3** | **К3** |
| УЗ 4 | **К3** | **К3** | **К4** |

**Сравнение получившихся значений по первой и второй классификации.**

В случае, если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение требований к ПДн. Соответствие:

|  |  |
| --- | --- |
| **Меры защиты информации предусмотренные классом защищенности ИС** | **Обеспечивают уровень защищенности персональных данных** |
| **К1** | 1, 2, 3 и 4 |
| **К2** | 2, 3 и 4 |
| **К3** | 3 и 4 |
| **К4** | 4 |

Примечание: Если есть подсистемы, использовать нижеприведенную структуру документа. Сегменты – объединения маленьких ИСПДн (Баз Данных) по общему функционалу и единому классу.

В связи с наличием в информационной системе <наименование ИСПДн><название организации> отдельных сегментов:

* ***<маркированный список названий систем>***

целесообразно проводить классификацию отдельных сегментов и всей системы в целом.

**Классификация сегмента <наименование сегмента ИСПДн><название организации>**

Данный сегмент включает в себя следующие информационные системы персональных данных:

* ***<маркированный список названий маленьких ИСПДн>***.

1. **Определение класса защищенности**

В соответствии с Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» комиссия установила следующее: ***<классификация по стандартной схеме>***.

1. **Определение уровня защищенности персональных данных**

В соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» комиссия установила следующее: ***<классификация по стандартной схеме>***.

Затем (соблюдая очередность систем и ту же структуру текста) провести классификацию каждого заявленного сегмента. И только в конце общий класс системы:

**Классификация ИСПДн <наименование ИСПДн><название организации>**

На основании полученных данных и в соответствии с Постановлением Правительства Российской Федерации №1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в информационной системе персональных данных <наименование ИСПДн><название организации> реализуемые меры защиты информации для информационной системы класса защищенности **К1** обеспечивают **1** уровень защищенности персональных данных.

1. **Вопросы**
2. Какие исходные данные необходимы для проведения классификации?
3. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
4. Какова специфика проведения классификации?
5. Каковы суть и содержание нормативной основы организации ЗСИ?

**Список дополнительной литературы:**

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»