**МИНОБРНАУКИ РОССИИ**

**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**

**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**

**Кафедра ИБ**

**ОТЧЕТ**

**по лабораторной работе №3**

**по дисциплине «Технология разработки ИС в ЗИ»**

**ТЕМА: Классифицирование ИС**

|  |  |  |
| --- | --- | --- |
| Студенты гр. 3361 |  | Воловик П. А. |
|  |  | Столетов А. С. |
|  |  | Субботин Д.А |
| Преподаватель |  | Березин А.Н. |

Санкт-Петербург

2018

**Цель работы**

Получить практические навыки классифицирования информационных систем персональных данных в соответствии с существующими требованиями.

Постановка задачи

Выполнить все шаги работы, необходимые для классифицирования ИС. Сформировать акт классификации на основе шаблона из приложения В.

Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Информацию следует классифицировать для:

1. определения потребности защитных мер;
2. расстановки приоритетов;
3. определения ожидаемой степени защиты информации.

*Классификация ИСПДн*

Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

**УТВЕРЖДАЮ**

Директор

ООО “НСТ”

Бобриков М.В.

«28» февраля 2018 г

**АКТ**

**классификации информационной системы персональных данных**

**«БД сотрудников ООО «НСТ»**

Комиссия в составе: начальник службы безопасности Воловик П.А; члены комиссии: администратор безопасности Столетов А.С., администратор безопасности Субботин Д.А., – в соответствии с приказом директора ООО “НСТ” Бобрикова М.В. «О комиссии по классификации информационной системы персональных данных «БД сотрудников ООО «НСТ»» от 25.02.2018 № 666, провела обследование информационной системы персональных данных (далее – ИСПДн) «БД сотрудников ООО «НСТ»».

По результатам проведенного анализа исходных данных ИСПДн   
«БД сотрудников «НСТ» были установлены следующие характеристики:

Таблица 1. Характеристики исследуемой ИС

|  |  |
| --- | --- |
| Категории субъектов персональных данных | Сотрудники организации |
| Категории обрабатываемых персональных данных | Общедоступные |
| Количество субъектов персональных данных (сотрудники) | Менее 100000 (не имеет значения, если речь о сотрудниках) |
| Тип актуальных угроз | Угрозы 2 типа |

На основании полученных данных, в соответствии с моделью угроз безопасности информации в ИСПДн «База данных сотрудников ООО «НСТ», согласно Постановлению правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" информационной системе персональных данных «БД сотрудников ООО «НСТ»» присвоен уровень защищенности УЗпдн3.

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственной тайну, содержащейся в государственных информационных системах», в таблице 2 были рассмотрены такие характеристики ИСПДн, как свойства информации, уровень значимости информации и масштаб ИСПДн.

Таблица 2. Определение масштаба и УЗИ исследуемой системы

|  |  |  |
| --- | --- | --- |
| Характеристика ИСПДН | | Степень ущерба |
| Свойство информации | Конфиденциальность | Низкая |
| Целостность | Средняя |
| Доступность | Средняя |
| Уровень значимости информации | Узи 2 | |
| Масштаб ИСПДН | Региональный | |

По результатам определения уровня значимости информации и масштаба информационной системы, комиссия определила класс защищенности информационной системы (К), в соответствии с таблицей 3:

Таблица 3. Определение класса защищенности

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости информации (УЗи) | Масштаб | | |
| Ф | Р | О |
| УЗи 1 | К1 | К1 | К1 |
| УЗи 2 | К1 | К2 | К2 |
| УЗи 3 | К2 | К3 | К3 |
| УЗи4 | К3 | К3 | К4 |
| **Присвоенный класс защищенности ИСПДн** | | | К2 |

|  |  |
| --- | --- |
| **Председатель комиссии:** |  |
| Начальник службы безопасности | \_\_\_\_\_\_\_\_\_\_\_ Воловик П.А. |
| **Члены комиссии:** |  |
| Администратор безопасности | \_\_\_\_\_\_\_\_\_\_\_ Столетов А.С. |
| Администратор безопасности | \_\_\_\_\_\_\_\_\_\_\_ Субботин Д.А. |

Согласно данному акту, рассматриваемой системе в результате классификации присвоен класс защищенности К2, а уровень защищенности УЗ-3.

При определении К2, данные опирались на факты об организации (масштаб системы), а также на специфику обрабатываемых данных (информация о системе). При определении уровня защищенности, помимо прочего, необходимо определить тип актуальных угроз. Это было сделано исходя из методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008), а также опираясь на данные исследований, проведенных в предыдущих работах, а именно на данные, представленные в таблице А19 лабораторной работы №1.

Согласно этой таблице у некоторых программ прикладного характера отсутствует сертификат, следовательно, такие программы, можно считать подверженными атакам нарушителей, в то время, как все системные программы имеют сертификаты и могут быть признаны защищенными.

Исходя из этой информации, можно сделать вывод, что в нашей системе актуальными угрозами считаются угрозы 2-го типа.

**Вывод**

В ходе данной работы была классифицирована исследуемая ИС.

Для этого были определены основные характеристики ИСПДн:

* Типы угроз информационной системы;
* Категория персональных данных, обрабатываемых в системе;
* Субъекты персональных данных и их количество;
* Уровень значимости информации;
* Масштаб ИСПДн.

В результате проведённого исследования системе был назначен уровень защищённости УЗпдн3, класс защищённости К2**.**

В соответствии с Приложением 2 к приказу ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственной тайну, содержащейся в государственных информационных системах» для данного класса защищенности 2 должны быть реализованы следующие меры защиты информации:

1. По группе мер идентификации и аутентификации субъектов и объектов доступа (далее ИАФ) – ИАФ.1 – ИАФ.6;
2. По группе мер управления доступом субъектов к объектам доступа (далее УПД) – УПД.1 – УПД.6, УПД.10, УПД.11, УПД.13 – УПД.17;
3. По группе мер ограничение программной среды (далее ОПС) – ОПС.2, ОПС.3;
4. По группе мер защиты машинных носителей информации (далее ЗНИ) – ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8;
5. По группе регистрации событий безопасности (далее РСБ) – РСБ.1 – РСБ.7;
6. По группе антивирусной защиты (далее АВЗ) – АВЗ.1, АВЗ.2;
7. По группе обнаружения вторжений (далее СОВ) – СОВ.1, СОВ.2;
8. По группе анализа защищенности информации (далее АНЗ) – АНЗ.1 – АНЗ.5;
9. По группе обеспечения целостности ИС и информации (далее ОЦЛ) - ОЦЛ.1, ОЦЛ.3, ОЦЛ.4;
10. По группе обеспечения доступности информации (далее ОДТ) – ОДТ.3 – ОДТ.5, ОДТ.7;
11. По группе защиты среды виртуализации (далее ЗСВ) – ЗСВ.1 – ЗСВ.4, ЗСВ.6 – ЗСВ.10;
12. По группе защиты технических средств – ЗТС.2 – ЗТС.4;
13. По группе защиты ИС, её средств, систем связи и передачи данных (далее ЗИС) – ЗИС.1, ЗИС.3, ЗИС.5, ЗИС.7 – ЗИС.9, ЗИС.11 – ЗИС.13, ЗИС.15, ЗИС.17, ЗИС.20, ЗИС.22 – ЗИС.24, ЗИС.30.

Ниже в приложении 1 приведен пример приказа о назначении комиссии по классификации ИСПДн, которая обязана назначаться (а значит и приказ обязан присутствовать как нормативный документ) при проведении классификации.

**Приложение А**

**УТВЕРЖДАЮ**

Директор ООО «НСТ»

Бобриков М.В.

26.02.2018 г

**Приказ**

**№666 от 25.02.18**

**О назначении комиссии по проведению классификации информационной системы «ИНФОБЕЗ».**

В связи с подготовкой информационной системы «ИНФОБЕЗ» к проведению классификации

**ПРИКАЗЫВАЮ:**

Создать комиссию по проведению сопровождению классификации информационной системы из числа сотрудников ООО «НСТ» в составе:

Председатель комиссии:

Начальник службы безопасности – Воловик П.А.

Члены комиссии:

Администратор безопасности – Столетов А.С.

Администратор безопасности – Субботин Д.А.

Комиссии руководствоваться документами:

1. ФСТЭК «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17.
2. Распорядительные акты ООО «НСТ».

Комиссии в срок до 01.03.2018 г.:

1. Проанализировать информационную систему и хранилища данных в ней;
2. Провести классификацию информационной системы в соответствии с приказом ФСТЭК «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17.
3. По результатам работ составить «Акт о классификации информационной системы персональных данных «БД сотрудников ООО «НСТ»

Контроль за исполнением приказа возложить на Воловика П.А. – начальника службы безопасности.

Директор ООО «НСТ» Бобриков М.В.

Список литературы

1. В. Н. Сабынин, А. Н. Березин, И. В. Ковалева, Технология разработки информационных систем в защищенном исполнении: лабораторный практикум. СПбГЭТУ «ЛЭТИ», 2016
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. 14.02.08 ФСТЭК России)
3. Методический документ ФСТЭК «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн»
4. [Положени](http://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-17112007-n-781/#100015)е об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Постановлением Правительства РФ от 17.11.07 №781)
5. Федеральный закон «О персональных данных» ФЗ-152