# Показатели защищенности средств вычислительной техники

Основы информационной безопасности

# Показатели и классы защищенности СВТ

- **Показатель защищенности средств вычислительной техники** (Показатель защищенности) (Protection criterion of computer systems) - характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.
- **Класс защищенности средств вычислительной техники, автоматизированной системы** (Protection class of computer systems) - определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

# Классы защищенности СВТ

- Согласно руководящему документу «*Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации*» устанавливается семь классов защищенности СВТ от НСД к информации.
- ***Самый низкий класс – седьмой, самый высокий – первый.***
- ***Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:***
  - первая группа содержит только один седьмой класс;
  - вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
  - третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
  - четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

# Классы защищенности СВТ

# Классы защищенности СВТ

- Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы. Перечень показателей по классам защищенности СВТ приведен в таблице.
- ***Обозначения:***
  - "-" – нет требований к данному классу;
  - "+" – новые или дополнительные требования,
  - "=" – требования совпадают с требованиями к СВТ предыдущего класса.

# Классы защищенности СВТ

| Наименование показателя | Класс защищенности | | | | | |
|---|---|---|---|---|---|---|
| | 6 | 5 | 4 | 3 | 2 | 1 |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчуждаемый физический носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство для пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Тестовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |

# Требования к защите СВТ

- Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации.
- Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.
- ***Требования к АС третьей группы***
- ***Обозначения:***
  - " - " - нет требований к данному классу;
  - " + " - есть требования к данному классу.

# Классы защищенности АС и категории информации ограниченного доступа

# Определение уровня защищенности персональных данных

Для определения уровня защищенности необходимо установить категории обрабатываемых персональных данных субъектов (физических лиц), вид обработки по форме отношений между субъектами и организацией, количество субъектов, а также тип угроз актуальных для информационной системы.

Категории обрабатываемых персональных данных (ПДн), подразделяются на 4 группы:

1 группа – **специальные категории ПДн**, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

2 группа – **биометрические ПДн**, то есть данные, характеризующие биологические или физиологические особенности субъекта, например фотография или отпечатки пальцев;

3 группа – **общедоступные ПДн**, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4 группа – **иные категории ПДн**, не представленные в трех предыдущих группах.

# Определение уровня защищенности персональных данных

По форме отношений между вашей организацией и субъектами обработка подразделяется на 2 вида:

- обработка персональных данных работников (субъектов, с которыми ваша организация связана трудовыми отношениями);
- обработка персональных данных субъектов, не являющихся работниками вашей организации.

По количеству субъектов, ПДн которых обрабатываются, нормативным актом определены лишь 2 категории:

- менее 100 000 субъектов;
- более 100 000 субъектов;

И наконец, типы актуальных угроз:

- угрозы 1-го типа связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;
- угрозы 2-го типа связанны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;
- угрозы 3-го типа не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн.

Как установить тип актуальных угроз не регламентировано, поэтому необходимо привлекать для оценки специалистов в области информационной безопасности.

# Определение уровня защищенности персональных данных

| Категории ПДн | | Специальные | | | Биомет-рические | Иные | | | Общедоступные | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Собственные работники | | нет | нет | да | | нет | нет | да | нет | нет | да |
| Количество субъектов | | более 100 тыс. | менее 100 тыс. | | | более 100 тыс. | менее 100 тыс. | | более 100 тыс. | менее 100 тыс. | |
| Тип актуальных угроз | 1 | **1 УЗ** | **1 УЗ** | **1 УЗ** | **1 УЗ** | **1 УЗ** | **2 УЗ** | **2 УЗ** | **2 УЗ** | **2 УЗ** | **2 УЗ** |
| | 2 | **1 УЗ** | **2 УЗ** | **2 УЗ** | **2 УЗ** | **2 УЗ** | **3 УЗ** | **3 УЗ** | **2 УЗ** | **3 УЗ** | **3 УЗ** |
| | 3 | **2 УЗ** | **3 УЗ** | **3 УЗ** | **3 УЗ** | **3 УЗ** | **4 УЗ** | **4 УЗ** | **4 УЗ** | **4 УЗ** | **4 УЗ** |

# Определение уровня защищенности персональных данных

4 уровень защищенности персональных данных (УЗ4) является самым минимальным уровнем из 4 (четырех) уровней установленных Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01.11.2012 №1119.

Под 4 уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

**Условия для определения 4-го уровня защищенности персональных данных**

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в ИСПДн устанавливается при наличии хотя бы одного из следующих условий:

# Определение уровня защищенности персональных данных

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в ИСПДн устанавливается при наличии хотя бы одного из следующих условий:

- для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает общедоступные персональные данные;
- для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

# Пример

Для прикладного ПО должна быть проверка на недокументированные возможности (отправляют они чего-то, куда-то без вашего ведома и вообще не живут-ли своей жизнью в сети). По окончании проверки на ПО выдают сертификат от ФСТЭК. Если в сети есть хоть одно ПО без сертификата ФСТЭК, то типом актуальных угроз можно считать тип 2 - "актуальные угрозы, связанные с наличием недокументированных возможностей в прикладном программном обеспечени". Если есть операционные системы без сертификата ФСТЭК, то тип 1 "актуальны угрозы, связанные с наличием недокументированных возможностей в системном программном обеспечении". А вот если в организации есть сотрудник, касающийся компьютеров и являющийся сыночком генерального директора, которому все можно и даже в КС на серваке поиграть, то тип 3 "актуальны угрозы, не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении". Я все так понял.