**Министерство образования и науки Самарской области**

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»**

**КОНТРОЛЬНАЯ РАБОТА**

**ПО ДИСЦИПЛИНЕ «Делопроизводство и режим секретности»**

**НА ТЕМУ: «Правовое регулирование защиты информации в правоохранительных органах»**

**Выполнил студент группы ПД-325**

**Баева Кристина**

**Проверил преподаватель по дисциплине**

**«Делопроизводство и режим секретности»**

**Варламова Марина Васильевна**

**Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Самара, 2018**

**Содержание**

Введение……………………………………………………………………………...3

1. Цели защиты информации……………………………………………4
2. Принципы защиты информации от несанкционированного доступа5
3. Методы и средства защиты информации……………………………..6

Заключение…………………………………………………………………………...8

Список использованной литературы……………………………………………….9

**Введение**

В Федеральном законе РФ «Об информации, информатизации и защите информации», принятом 25 января 1995 года Государственной Думой, определено, что «информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления».

Информация имеет ряд особенностей: она нематериальна, хранится и передается с помощью материальных носителей, любой материальный объект содержит информацию о самом себе или о другом объекте.

Защита информации - это перечень мероприятий, направленных на достижение полной безопасности и защищенности сведений с целью предотвращения утечки информации.

1. **Цели защиты информации**

Основными целями защиты информации являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;

- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;

- сохранение государственной тайны, конфиденциальности документированной информации.

1. **Принципы защиты информации от несанкционированного доступа**

Закрытие каналов несанкционированного получения информации должно начинаться с контроля доступа пользователей к ресурсам ИС. Эта задача решается на основе ряда принципов:

**Принцип обоснованности доступа,** заключается в обязательном выполнении следующего условия: пользователь должен иметь достаточную форму допуска для получения информации, требуемого им уровня конфиденциальности с тем, чтобы выполнить заданные производственные функции.

**Принцип разграничения,**  для предупреждения нарушения безопасности информации, которое, например, может произойти при записи секретной информации на несекретные носители и в несекретные файлы, при передаче ее программам и процессам, не предназначенным для обработки секретной информации, а также при передаче секретной информации по незащищенным каналам и линиям связи, необходимо осуществлять соответствующее разграничение потоков информации и прав доступа к этой информации

**Принцип чистоты ресурсов,** заключается в очистке ресурсов, содержащих конфиденциальную информацию, при их удалении или освобождении пользователем до перераспределения этих ресурсов другим пользователям.

**Принцип персональной ответственности,** каждый пользователь ИС должен нести персональную ответственность за свою деятельность в системе, включая любые операции с секретной информацией и возможные нарушения ее защиты – случайные или умышленные действия, которые приводят или могут привести к НСД или, наоборот делают такую информацию недоступной для законных пользователей

**Принцип целостности средств защиты,** подразумевает, что средства защиты информации в ИС должны точно выполнять свои функции в соответствии с перечисленными принципами и быть изолированными от пользователей.

1. **Методы и средства защиты информации**

Существуют следующие методы защиты информации:

- препятствие - метод физического преграждения пути злоумышленнику к защищаемой информации;

- управление доступом - метод определения и распределения ресурсов системы санкционированным пользователям;

- шифрование - метод защиты информации в коммуникационных каналах путем ее криптографического закрытия;

- регламентация - метод защиты информации, создающий специальные условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму;

- принуждение - такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности;

- побуждение - метод защиты информации, который стимулирует пользователя и персонал системы не нарушать установленных норм (высокая зарплата).

Средства защиты информации:

- физические средства - механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов;

- аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации;

- программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации;

- организационные средства - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации;

- законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности;

- психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

Нормативно-правовая база защиты информации в ОВД основывается на Конституции, Федеральных законах, уголовном и гражданском законодательстве Росси.

Среди законов выделяют базовый для информационной сферы федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Особое место среди нормативных актов, регулирующих отношения по поводу информации, принадлежит закону РФ от 21.07.1993 № 5485 – 1 «О государственной тайне».

**Заключение**

Организационные и правовые (законодательные) средства защиты информации являются наиболее универсальными, поскольку принципиально могут быть применены для каналов несанкционированного доступа к информации в любых автоматизированных системах.

Трудно представить эффективное применение других средств защиты информации без соответствующей нормативно-правовой базы. К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К ним же относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных соглашений.

Закон определяет защиту информации, как принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

**Список использованной литературы**

1. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации от 27 июля 2006 г. №149-ФЗ».

2. Закон РФ от 21 июля 1993 г. №5485-I «О государственной тайне» (в ред. Федерального закона от 18 июля 2009 г. №180-ФЗ).

3. <https://www.securitylab.ru/>

4. <https://studfiles.net/>

5. <https://studopedia.su/>