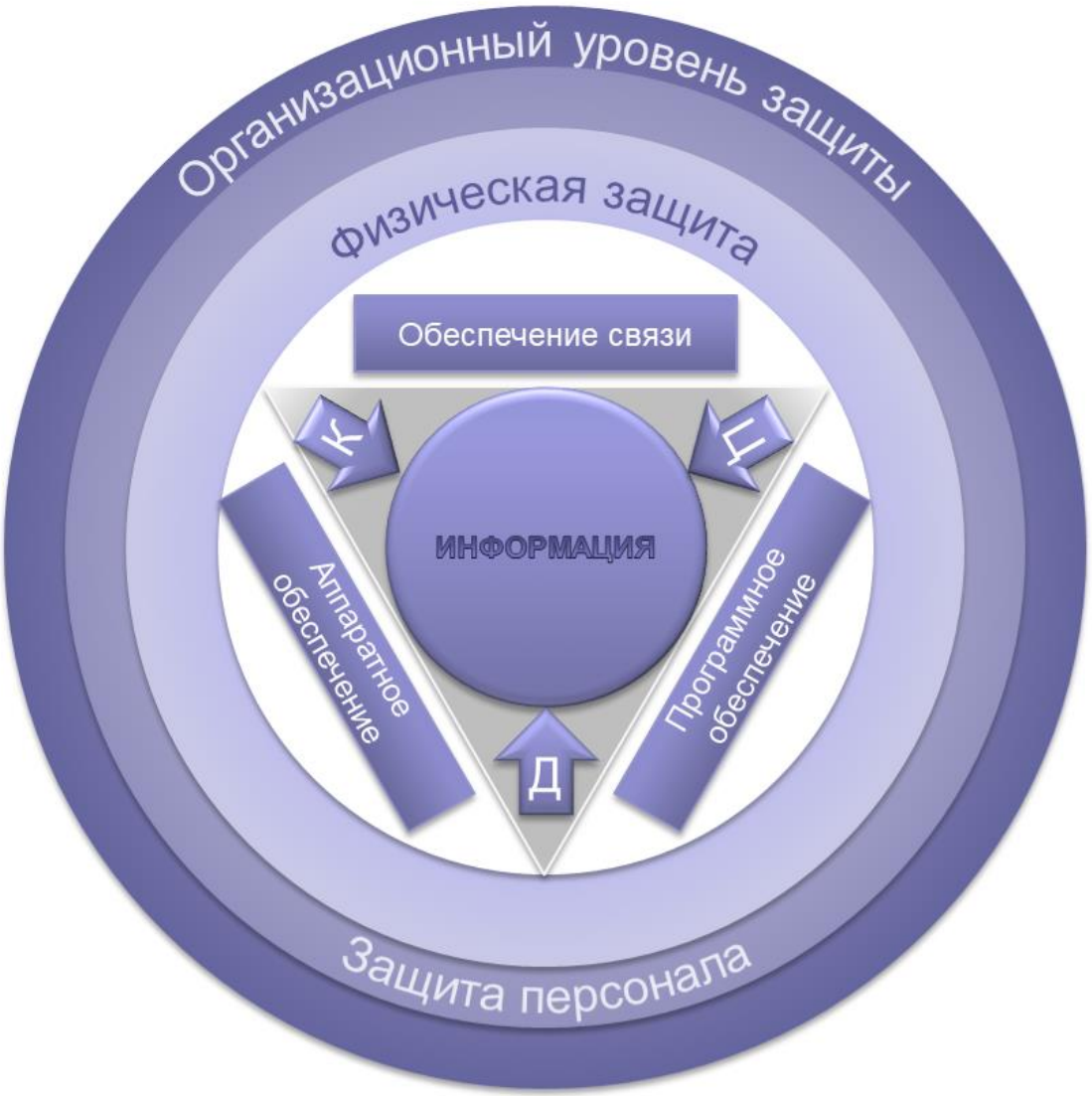
Информационная безопасность Методы защиты информации

Информационной безопасностью называют комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

- ***конфиденциальность*** информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц);
- ***целостность*** информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения);
- ***доступность*** информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц);
- ***учет*** всех процессов, связанных с информацией.



Обеспечение **безопасности информации** складывается из трех составляющих:

- Конфиденциальности,
- Целостности,
- Доступности.

Точками приложения процесса защиты информации к информационной системе являются:

- аппаратное обеспечение,
- программное обеспечение
- обеспечение связи (коммуникации).

Сами процедуры(механизмы) защиты разделяются на

- защиту физического уровня,
- защиту персонала
- организационный уровень.

Нормативная база по защите ПД

- Конституция РФ
- Федеральные законы
- Постановления Правительства Российской Федерации
- Документы уполномоченных федеральных органов в виде приказов, положений, требований, методик и рекомендаций (открытые и ограниченного доступа)

Законодательство о персональных данных

- ФЗ «**Об информации, информационных технологиях и о защите информации**» №149-ФЗ от 27 июля 2006 года
- ФЗ «**О персональных данных**» №152-ФЗ от 27 июля 2006 года
- ФЗ **«О лицензировании отдельных видов деятельности»** №128-ФЗ от 8 августа 2001 года
- **Трудовой кодекс Российской Федерации** № 197-ФЗ от 30 декабря 2001 года (глава 14)
- **Кодекс Российской Федерации об административных правонарушениях** № 195-ФЗ от 30 декабря 2001 года (Статья 13.11.)
- ФЗ **«О государственной гражданской службе Российской Федерации»** № 79-ФЗ от 27 июля 2004 года (Глава 7)
- ФЗ **«О муниципальной службе в Российской Федерации»** № 25-ФЗ от 2 марта 2007 года (Статья 29)

Подзаконные нормативные акты Правительства РФ

- Постановление Правительства РФ от 17 ноября 2007 г. № 781 «**Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных**»
- Постановление Правительства РФ от 6 июля 2008 г. № 512 «**Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных**»
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «**Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации**»

Методические документы ФСТЭК («ДСП»)

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных»
- «Рекомендации по обеспечению безопасности персональных данных при обработке при их обработке в информационных системах персональных данных»

Методические документы ФСБ

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

Перечень основных рабочих документов по информационной безопасности

- Положение о защите персональных данных
- Приказ о назначении лиц, ответственных за обработку ПДн
- Перечень персональных данных, подлежащих защите
- Политика информационной безопасности
- Положение о разграничении прав доступа к обрабатываемым персональным данным
- Приказ о проведении внутренней проверки
- Отчет о результатах проведения внутренней проверки

Государственные органы, регулирующие вопросы использования и защиты персональных данных

- **Роскомнадзор** (федеральная служба по надзору в сфере связи и массовых коммуникаций), является основным исполнительным и надзорным органом по защите прав физических лиц, чьи персональные данные обрабатываются. http://www.rsoc.ru и http://pd.rsoc.ru

- **ФСТЭК России** (Федеральная служба по техническому и экспортному контролю РФ) – лицензирование деятельности операторов персональных данных при осуществлении ими технической защиты конфиденциальной информации. http://www.fstec.ru

- **ФСБ России** (Федеральная служба безопасности РФ) традиционно контролирует деятельность операторов персональных данных, при использовании ими при защите персональных данных криптографических средств защиты. http://www.fsb.ru

Парольная политика

- Пароли системных учетных записей (администратора домена, локального администратора, root и т. д.) должны изменяться ежеквартально.
- Срок действия паролей учетных записей домена должен составлять не более 6 месяцев. Рекомендуемый интервал смены пароля 3 месяца.
- Пароль учетной записи пользователя, имеющего административные привилегии, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.
- Запрещается передача паролей пользователям при помощи почтовых сообщений либо иным другим открытым способом через Интернет.
- Пароль полученный пользователем, необходимо сменить при первом входе в систему.

Параметры сильных паролей

- Содержит сочетание букв верхнего и нижнего регистров (например, a-z, A-Z).
- Включает цифры и знаки пунктуации, например, 0-9, !@#$%^&*()_+|~-=\`{}[[ ]]:«;'<>?,./).
- Состоит из восьми и более символов.
- Не является словом на любом языке, диалекте, сленге, жаргоне и т.д.
- Не основан на пресональной информации, например фамилии, дате рождения и т.д.
- Никогда не записывается и не хранится on-line.

Хранение паролей

- Запрещается хранить пароли в открытом виде (на столе, под клавиатурой, приклеенным к монитору)
- Необходимо вести журнал учета выдачи паролей
- Пароли на бумажном носителе хранятся в опечатанных конвертах
- Конверты с паролями и журнал хранятся у начальника отдела в сейфе или запираемом железном шкафу