

ВУЗ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему:

«Методика и инструментальные средства создания документов по защите персональных данных в информационных системах»

Выполнена:

Научный руководитель:

Цель и задачи

Цель - оценка методов и инструментальных средств создания документов по защите персональных данных в информационных системах.

Задачи:

1. Рассмотрение основ защиты персональных данных.
2. Изучить методы защиты персональных данных.
3. Рассмотреть процесс создания документации по защите персональных данных.
4. Рассмотреть реализацию базы данных для защиты персональных данных.

Деструктивные действия

Нанесение вреда программному обеспечению и пользовательским данным.

Повреждение встроенного ПО, данных и драйверов устройств в системе персональных данных.

Нанесение вреда программам, данным и драйверам устройств, ответственным за загрузку операционной системы и функционирование средств информационной безопасности.

Нанесение вреда программам и данным специализированного программного обеспечения.

Внедрение вредоносных программ, аппаратных и программных закладок и тому подобное.

Влияние на инструменты управления конфигурацией сети.

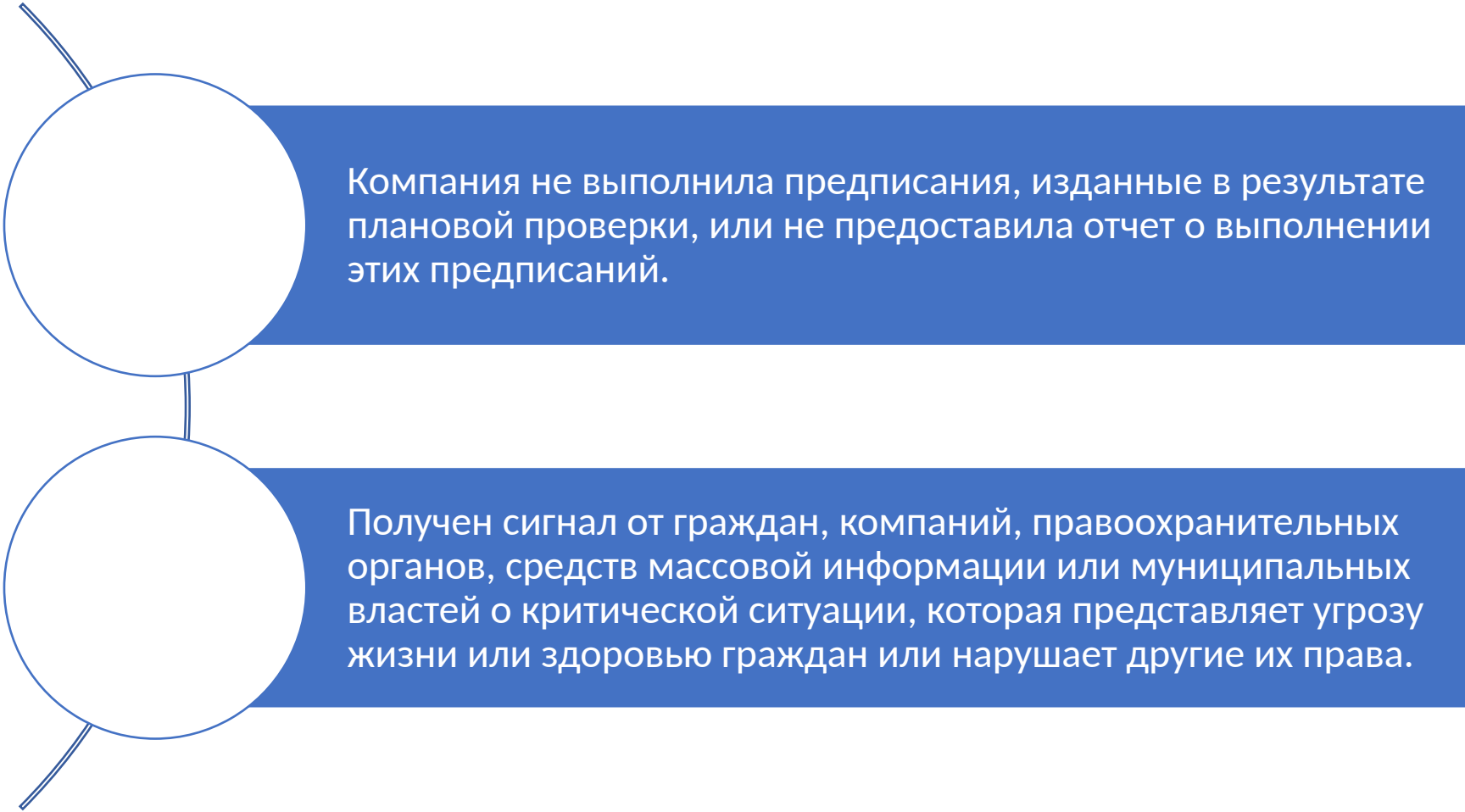
Нанесение ущерба средствам защиты информации.

Для проведения внеплановой проверки должны быть выполнены два условия:

Наличие информации о существенном нарушении закона, жалобах или истечении срока, предусмотренного для исправления ранее допущенных нарушений.

Получение согласия областной прокуратуры на проведение контрольных мероприятий.

Внеплановая проверка может быть проведена только в серьезных случаях:



Компания не выполнила предписания, изданные в результате плановой проверки, или не предоставила отчет о выполнении этих предписаний.

Получен сигнал от граждан, компаний, правоохранительных органов, средств массовой информации или муниципальных властей о критической ситуации, которая представляет угрозу жизни или здоровью граждан или нарушает другие их права.

Результаты аудита

Подготовка отчета о проверке и его направление в организацию.

Выдача предписания об устранении выявленных нарушений закона.

Привлечение оператора к административной ответственности.

Выдача приказа о приостановлении деятельности.

Направление мотивированного заключения в правоохранительные органы с просьбой привлечь сотрудников оператора к уголовной ответственности

Категории субъектов, которые могут нанести ущерб охраняемым законом интересам

Граждане России,
преследующие свои
личные цели.

Иностранные
разведывательные
службы.

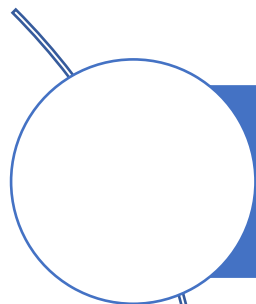
Другие иностранные
организации, будь то
террористические или
коммерческие
структуры.

Преступные
группировки

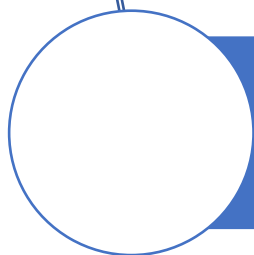
Анализ угроз

Угрозы	Анализ
Внутренние угрозы (инсайдерские)	Эти риски возникают, когда внутренний пользователь, имеющий доступ к информационным системам в рамках своего служебного положения, работы в компании или государственной структуре, может похитить или изменить данные.
Внешние	В этом случае субъект угрозы получает несанкционированный доступ к защищаемому объекту, используя возможности общедоступных сетей.
Технические	Эти угрозы возникают при использовании аппаратных закладок и программ, разработанных для кражи электронной информации

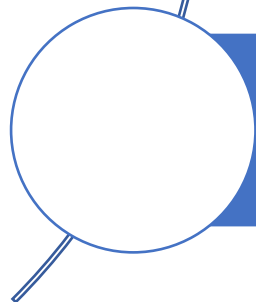
При подготовке этого документа рекомендуется использовать следующие документы в качестве руководства:



Постановление Правительства Российской Федерации от 01.10.2012 № 1119;



Методика определения фактических 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

Выводы

Реализация базы данных для защиты персональных данных играет решающую роль в обеспечении конфиденциальности, целостности и доступности информации о пользователях.

База данных предоставляет структурированное и централизованное хранилище для персональных данных, где информация может быть управляема и контролируема. Это позволяет упорядочить данные и обеспечить единый и точный источник информации о пользователях.

Реализация базы данных для защиты персональных данных является необходимым шагом для обеспечения безопасности и конфиденциальности информации о пользователях. Это помогает предотвратить утечку данных, минимизировать риски нарушений безопасности и обеспечить соблюдение законодательных требований, связанных с персональными данными.

СПАСИБО ЗА ВНИМАНИЕ!