V ЮБИЛЕЙНЫЙ СЪЕЗД
МЕДИЦИНСКИХ
СТАТИСТИКОВ
ГОРОДА МОСКВЫ

Современные методы обеспечения информационной безопасности при работе со статистическими данными

Департамент здравоохранения города Москвы

НИИ ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ И МЕДИЦИНСКОГО МЕНЕДЖМЕНТА

Содержание презентации

- Основные методы обеспечения информационной безопасности
- Угрозы информационной безопасности при работе со статистическими данными
- Требования к системе защиты при работе в ГИС, ИСПДН
- Недопущение утечки информации ограниченного доступа при работе со статистическими данными

Основные методы обеспечения информационной безопасности

Методы обеспечения информационной безопасности

Правовой

Совокупность законодательных актов, нормативно правовых документов, положений, инструкций, руководств требования которых являются обязательными в области защиты информации

Организационный

Совокупность мер, мероприятий и действий направленных на обеспечение должного уровня информационной безопасности в процессе работы с защищаемой информацией

Инженерно-технический

Совокупность специальных технических средств и мероприятий по их эксплуатации в целях обеспечения защиты информации

Правовой метод обеспечения информационной безопасности

Структура правовой защиты информации

- Международное право
  - Договоры конвенции, декларации
  - Патенты
  - Авторские права
  - Лицензии
- Внутригосударственное право
  - Государственные
    - Конституции
    - Законы
    - Указы
    - Постановления
  - Ведомственные
    - Приказы
    - Руководства
    - Положения
    - Инструкции

Организационной метод обеспечения информационной безопасности

Создание структурного подразделения по обеспечению информационной безопасности
Подразделение должно обязательно состоять из специалистов организационно- правового и инженерно-технического обеспечения.

Организация работы с сотрудниками (ознакомление с сотрудников, их обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)

Организация работы с документами и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)

Организация использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

Организация работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

Организация работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Инженерно-технический метод обеспечения информационной безопасности

Классификация инженерно - технического метода

Аппаратные	Программные	Криптографические
Аппаратные средства защиты информации и информационных систем реализованы на аппаратном уровне. Это разные по типу устройства (механические, электромеханические, электронные)	Специальные программы и программные комплексы, предназначенные для защиты информации	Аппаратно-программные и программные средства шифрования.

Инженерно-технический метод обеспечения информационной безопасности

Виды инженерно – технических средств

Аппаратные

- От несанкционированного доступа
- От утечки сведений, спровоцированной ПЭМИН
- От утечки речевой информации
- Защита телефонных линий
- Средства гарантированного уничтожения информации

Программные

- Встроенные средства защиты
- Программы-антивирусы
- Программы от несанкционированного доступа
- Межсетевые экраны
- Программы тестового контроля

Криптографические

- Программные СКЗИ
- Программно-аппаратные СКЗИ

Актуальные угрозы информационной безопасности при работе с данными

- Угроза утечки информации в социальных сетях , мессенджерах, электронной почте
- Бесконтрольное использование машинных носителей
- Несанкционированный доступ к конфиденциальной информации при использовании периферийных устройств (принтеры, МФУ и д.р.)
- Угроза компьютерных вирусов и вредоносных программ.
- Угроза утечки реквизитов доступа (логин и пароль) к информационной системе или к компьютеру пользователя где циркулируют данные.
- Угроза атаки с использованием социальной инженерии
- Бесконтрольный просмотр страниц в интернете
- Угроза утечки информации при использовании личного мобильного телефона или планшета при работе с данными
- Угроза несанкционированного доступа к информации при неавтоматизированной обработке данных

Требования к системе защиты

Требования к системе защиты регулируются следующими нормативно правовыми актами:

- ИСПДн - Постановление Правительства №1119 и приказ ФСТЭК России №21
- ГИС, с ПДн - приказ ФСТЭК России №17, Постановление Правительства №1119 и приказ ФСТЭК России №21

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 1 ноября 2012 г. № 1119

МОСКВА

Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

В соответствии со статьей 19 Федерального закона "О персональных данных" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые требования к защите персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

Председатель Правительства Российской Федерации Д.Медведев

ЗАРЕГИСТРИРОВАНО

Регистрационный № 28375

от 14 мая 2013

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

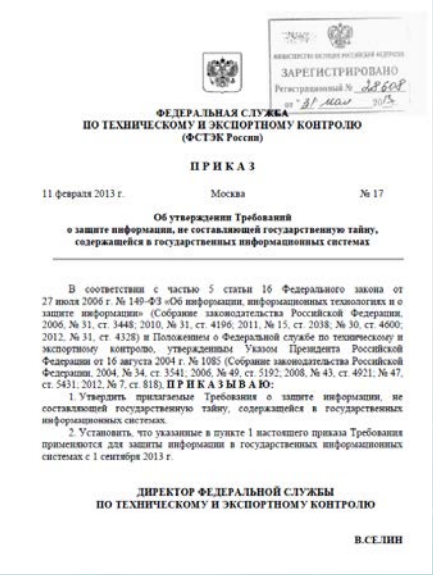
П Р И К А З

«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818), **П Р И К А З Ы В А Ю :**

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.



ЗАРЕГИСТРИРОВАНО

Регистрационный № 28608

от 31 мая 2013

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

П Р И К А З

11 февраля 2013 г. Москва № 17

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818), **П Р И К А З Ы В А Ю:**

1. Утвердить прилагаемые Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2. Установить, что указанные в пункте 1 настоящего приказа Требования применяются для защиты информации в государственных информационных системах с 1 сентября 2013 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Примеры требований к системе защиты

1. Идентификация и аутентификация субъектов доступа и объектов доступа;
2. Управление доступом субъектов доступа к объектам доступа;
3. Ограничение программной среды;
4. Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
5. Регистрация событий безопасности;
6. Антивирусная защита;
7. Обнаружение (предотвращение) вторжений;
8. Контроль (анализ) защищенности персональных данных;
9. Обеспечение целостности информационной системы и персональных данных;
10. Обеспечение доступности персональных данных;
11. Защита среды виртуализации;
12. Защита технических средств;
13. Защита информационной системы, ее средств, систем связи и передачи данных;
14. Выявление инцидентов
15. Управление конфигурацией

Недопущение утечки информации ограниченного доступа при работе со статистическими данными

Парольная защита:

- Никогда не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним.
- Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.
- Не используйте простые пароли, например: "12345, 123qwe321, 10121980" и т.п. Пароли должны быть не менее 8 символов, содержать прописные и строчные буквы (a-z, A-Z), цифры и спецсимволы (&*!%).
- Не используйте личные пароли (от соцсетей, личной почты и т.п.) для служебных информационных систем и наоборот, не используйте служебные пароли для личных целей.
- При временном оставлении своего рабочего места в обязательном порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».

Недопущение утечки информации ограниченного доступа при работе со статистическими данными

Антивирусная защита:

- Никогда не отключайте установленное на рабочем компьютере антивирусное программное обеспечение
- Обязательно проверяйте на наличие вирусов все внешние носители (дискеты, диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений Организации и т.п.)
- Во всех случаях возможного проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом сотруднику техподдержки или в отдел ИБ
- Если антивирус перестал обновляться или вовсе работать (на иконке антивируса появились восклицательные знаки, крестики или выдаются об этом сообщения на экране), то обязательно об этом сообщите ИТ - специалисту. Не отключайте антивирус!

Недопущение утечки информации ограниченного доступа при работе со статистическими данными

Интернет и электронная почта:

- Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.
- Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.
- Не передавать по электронной почте Ваши пароли а так же информацию ограниченного доступа.
- Перешлите подозрительное письмо ИБ/ИТ - специалисту для антивирусной проверки, не открывайте вложения самостоятельно.
- Не храните реквизиты доступа (логин и пароль) в браузере

Недопущение утечки информации ограниченного доступа при работе со статистическими данными

Социальные сети:

- Никогда не публикуйте информацию ограниченного доступа в социальных сетях
- Используйте разные пароли для соцсети и для электронной почты, которую указываете в социальной сети.
- Не указывайте рабочую почту при регистрации в социальной сети
- Проявляйте осторожность при переходе по ссылкам, полученным в сообщениях от других пользователей, если вы не знакомы с отправителем.
- При завершении работы в социальной сети осуществите выход из своего аккаунта
- При работе в социальной сети обязательно проверьте работоспособность антивируса.

Недопущение утечки информации ограниченного доступа при работе со статистическими данными

Мессенджеры:

- Не используйте иностранные сервисы для рабочей переписки
- Ограничьте использование мессенджера на рабочем компьютере
- Не обменивайтесь информацией ограниченного доступа в чатах мессенджера
- С подозрением относитесь к полученным ссылкам и файлам, даже если они поступили от известного отправителя. Прежде чем переходить по ссылке или открывать файл, узнайте другим способом связи, действительно ли ваш коллега (знакомый) отправлял их.
- Не делать скриншотов или других копий информации из чата
- Настройте двухфакторную аутентификацию в приложении мессенджера предварительно завершив активные сессии на других устройствах
- Отключите автозагрузку файлов

Правовое регулирование

Роскомнадзор напомнил, что 1 марта 2023 года вступили в силу ч. 8-10 ст. 10 Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Информация Роскомнадзора от 1 марта 2023 г.)

1 марта 2023 года

1 марта 2023 года вступают в силу ч. 8-10 ст. 10 закона «Об информации, информационных технологиях и о защите информации».

Закон устанавливает запрет для ряда российских организаций на использование иностранных мессенджеров (принадлежащих иностранным лицам информационных систем и программ для ЭВМ, которые предназначены и (или) используются для обмена сообщениями исключительно между их пользователями, при котором отправитель определяет получателей сообщений и не предусматривается размещение интернет-пользователями общедоступной информации в интернете).

По состоянию на 1 марта 2023 года к таким сервисам могут быть отнесены:

1. Discord;
2. Microsoft Teams;
3. Skype for Business;
4. Snapchat;
5. Telegram;
6. Threema;
7. Viber;
8. WhatsApp;
9. WeChat.

Просим российские организации учитывать новые обстоятельства при планировании своей деятельности.

27 июля 2006 года № 149-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Принят
Государственной Думой
8 июля 2006 года

Одобрен
Советом Федерации
14 июля 2006 года

Список изменяющих документов
(в ред. Федеральных законов от 27.07.2010 № 227-ФЗ, от 06.04.2011 № 65-ФЗ, от 21.07.2011 № 252-ФЗ, от 28.07.2012 № 139-ФЗ, от 05.04.2013 № 50-ФЗ, от 07.06.2013 № 112-ФЗ, от 02.07.2013 № 187-ФЗ, от 28.12.2013 № 396-ФЗ, от 28.12.2013 № 398-ФЗ, от 05.05.2014 № 97-ФЗ, от 21.07.2014 № 222-ФЗ, от 21.07.2014 № 242-ФЗ, от 24.11.2014 № 364-ФЗ, от 31.12.2014 № 531-ФЗ, от 29.06.2015 № 188-ФЗ, от 13.07.2015 № 263-ФЗ, от 13.07.2015 № 264-ФЗ, от 23.06.2016 № 208-ФЗ, от 06.07.2016 № 374-ФЗ, от 19.12.2016 № 442-ФЗ, от 01.05.2017 № 87-ФЗ, от 07.06.2017 № 109-ФЗ, от 18.06.2017 № 127-ФЗ, от 01.07.2017 № 156-ФЗ, от 29.07.2017 № 241-ФЗ, от 29.07.2017 № 276-ФЗ, от 29.07.2017 № 278-ФЗ, от 25.11.2017 № 327-ФЗ, от 31.12.2017 № 482-ФЗ, от 23.04.2018 № 102-ФЗ, от 29.06.2018 № 173-ФЗ, от 19.07.2018 № 211-ФЗ, от 28.11.2018 № 451-ФЗ, от 18.12.2018 № 472-ФЗ, от 18.03.2019 № 30-ФЗ, от 18.03.2019 № 31-ФЗ, от 01.05.2019 № 90-ФЗ, от 02.12.2019 № 426-ФЗ, от 02.12.2019 № 427-ФЗ, от 03.04.2020 № 105-ФЗ, от 08.06.2020 № 177-ФЗ)

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим

Спасибо за внимание !!!