Информационная безопасность

или

Темная сторона силы

Марковнин
Владимир Рудольфович

Часть первая. Официальная.

Законы

- 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»
  - Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
- 149-ФЗ «Об информации, информационных технологиях и защите информации»
  - регулирует отношения, возникающие при:
    - осуществлении права на поиск, получение, передачу, производство и распространение информации;
    - применении информационных технологий;
    - обеспечении защиты информации.

Подзаконные акты

- Постановление правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Подзаконные акты - 2

- Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Подзаконные акты - 3

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Заместитель директора ФСТЭК России 15 февраля 2008 г.)
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Заместитель директора ФСТЭК России 14 февраля 2008 г.)

Законные определения

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

Защита информации

- Защита информации представляет собой 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.

Что такое угроза?

- Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Три типа угроз

1. наличие недокументированных возможностей в системном программном обеспечении
2. наличие недокументированных возможностей в прикладном программном обеспечении
3. наличие недокументированных возможностей в системном и прикладном программном обеспечении

Критерии 4 уровней защиты персональных данных

- Тип угроз (предыдущий слайд еще можно вернуть :-))
- Тип персональных данных (специальные, биометрические, общедоступные, иные категории)
- Количество данных (порог — 100 000)

Данные о здоровье — это первый уровень защиты!!!

Как защищать (класс 4)

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Как защищать (класс 3)

- см. выше +
- назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе

Как защищать (класс 2)

- см. выше и выше +
- Ограничить доступ к содержанию электронного журнала сообщений исключительно кругом должностных лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей

Как защищать (класс 1)

- см. выше, выше и выше +
- автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;
- создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Состав и содержание мер по обеспечению безопасности персональных данных

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;

Состав и содержание мер по обеспечению безопасности персональных данных

- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Часть вторая. Интересная.

Авторизация ≠ Аутентификация

- Аутентифицироваться — доказать, что ты это ты
- Авторизоваться — получить право делать то, что имеешь право делать

Хороший пароль — сложный пароль,
...который трудно забыть

- Числа + буквы + разный регистр + спецсимволы
- Мнемонические пароли
- Визуальные пароли
- Генераторы паролей (http://genpas.peter.am)
- Программы для хранения паролей
- Двухуровневая аутентификация
- Oauth, open-ID
- Хэширование с солью

Синдром Раскольникова

- Права пользователя
- Права групп пользователей
- Права на уровне файловой системы

Концепция rwx

- R — чтение
- W — запись
- X — выполнение

- Пользователь
- Группа
- Остальные

Пример:

-r--------

Владелец имеет право чтения;
никто другой не имеет права выполнять никакие действия

-rwxr-xr-x

Каждый пользователь имеет право читать
и запускать на выполнение;
владелец может редактировать

Вредоносное ПО

- Вирусы
- Черви
- Программы для рассылки спама
- Троянские программы
- Кейлогеры
- Руткиты

Диагностика

- Антивирусное ПО
- Визуальный контроль

Лечение

- Антивирусное ПО
- Ручное удаление

Профилактика

- Не надеяться на антивирус
- Не переходить по подозрительным ссылкам
- Не устанавливать подозрительное ПО
- Не открывать флэшки даблкликом
- Пользоваться файловым менеджером
- Обновлять систему

Популярное вредоносное

- Autorun.inf
- Скрытие папок с созданием ссылок
- Win-локеры
- Двойное расширение файлов (image.jpg.exe)
- Социальная инженерия

- Страфиствуйтэ, я таджикский вирюс. Па причина ужасный бедность моей создателя и низкий уровне развитиё технология в наша страна я не способин причинять какая-либа уред Вашей компютеру. Поэтому ощень прашу Уас, пажальста, сами сатрите какая-нибут важная для Уас файлу, а патом разашлиты миня па почьта или аска другой адрисатам. Зарания благадарная за панимании и сатрудничесва.

- тут кто то твоё фото выложил *ROFL* http: //obnoklassniki.eu/?st.cmd=viewUserPhoto

Антивирусы

- Сравнение с базой
- Эвристический анализ
- Проактивная защита

Стена огня или межсетевые экраны

- Фильтрация трафика по правилам
- Анализ трафика
- Ведение списков ПО

Шифрование

- Шифрование файлов
- Шифрование файловой системы
- Шифрование трафика
- Цифровая подпись и шифрование

Подпиши меня цифрой

- Идентификация автора
- Подтверждение неизменности документа
- Ограничение доступа к документу
- Закрытый ключ
- Открытый ключ
- Центр сертификации
- Списки отзыва

06.04.2011 N 63-ФЗ «Об электронной подписи»

Fishing
или
как поймать миллион

- Цель — создать похожее, чтобы получить недоступное.

Сетевой фарш
или
средства борьбы со спамом

- Ведение списков
- Настройка фильтров
- Алгоритмы Байеса
- Хранение контактов в тайне

Благодарю за внимание

ВОПРОСЫ?

E57cbf5d50623c957d75dc2def25c19a
0148dd920fe7d3d69089c8e7ad81e199