ЭЛВИС-ПЛЮС

Особенности классификации информационных систем, обрабатывающих персональные данные в страховых компаниях

(мнение эксперта)

Сергей ВИХОРЕВ
Заместитель Генерального директора по развитию
ОАО «ЭЛВИС-ПЛЮС»

2009 год

ЭЛВИС-ПЛЮС

Вопросы презентации

- Что требует закон
- Что надо классифицировать
- Особенности обработки ПДн I-ой категории
- Какие риски возможны
- Можно ли снизить класс защиты

ЭЛВИС-ПЛЮС

Вместо эпиграфа

Фобия — сильный иррациональный страх определенных предметов или ситуаций (например, высоты или замкнутого пространства, привлечения к себе внимания других)

Н. Д. Творогова
Клиническая психология

Фобия (от греч. phóbos – страх, боязнь), часть сложных слов, выражающая боязнь чего-либо, страх перед чем-либо, например гидрофобия, клаустрофобия

БСЭ

Законофобия – иррациональный страх перед последствиями вступления в силу закона «О персональных данных»

С. В. Вихорев
Практический опыт

ЭЛВИС-ПЛЮС

ПРОЛОГ

В соответствии с Законом «О персональных данных» организация или физическое лицо, осуществляющее и/или организующее обработку персональных данных, является оператором персональных данных и обязано обеспечить их защиту.

До 1 января 2010 года все операторы обязаны обеспечить защиту персональных данных.

В декабре 2009 года в первом чтении принят Федеральный закон о внесении изменений в Закон «О персональных данных»:

ИСПдн, созданные до 1.01.2010 года должны быть приведены в соответствие не позднее 01.01.2011 года

РАССЛАБЛЯТЬСЯ НЕЛЬЗЯ!

Времени может, как всегда, не хватить!

ЭЛВИС-ПЛЮС

Что надо сделать?

Обязанности операторов ПДн

- **Установить необходимость обработки ПДн**
- **Провести инвентаризацию ИР, определить перечень ПДн**
- **Урегулировать правовые вопросы обработки ПДн**
- **Направить в Роскомнадзор уведомление** *(при необходимости)*
- **Разработать модель угроз**
- **Провести классификацию ИСПДн**
- **Получить лицензию на деятельность по ТЗИ** *(не для всех)*
- **Определить требования по защите ПДн**
- **Спроектировать Систему защиты ПДн и реализовать проект**
- **Провести оценку соответствия ИСПДн требованиям**
- **Организовать контроль соблюдения использования СЗИ**

ЭЛВИС-ПЛЮС

На какие ИС надо обратить внимание?

Рекомендации по инвентаризации ИР страховых компаний

- ✓ **ИС обработки ПДн клиентов страховых компаний**
  - ОСАГО
  - КАСКО
  - ОМС
  - «Зеленая Карта»
  - Обмена информацией с РСА и другими организациями
- ✓ **ИС обработки ПДн персонала страховых компаний**
  - Система кадрового учета
  - Система расчета оплаты труда
  - Система учета абонентов корпоративной АТС
- ✓ **Специальные и служебные ИС, могущие обрабатывать ПДн**
  - Система взаимодействия с брокерами компании
  - Служба учета прав доступа пользователей корпоративных ИР
  - Служба каталогов корпоративной ИС
  - Система контроля и управлением доступом на объекты

ЭЛВИС-ПЛЮС

Как правильно классифицировать ИСПДн?

Рекомендации по созданию СЗПДн

Классификация необходима для определения *перечня организационных и технических мероприятий*, необходимых для *обеспечения безопасности* ПДн. Проведение классификации позволяет реализовать дифференцированный подход к обеспечению безопасности ПДн в зависимости от объема обрабатываемых ПДн и угроз безопасности и минимизировать затраты на защиту ИСПДн

Классификация ИСПДн проводится операторами, организующими и осуществляющими обработку ПДн, а также определяющими цели и содержание обработки ПДн.

ЭЛВИС-ПЛЮС

По каким критериям оценивать ИС?

Рекомендации по классификации ИСПДн страховых компаний

- ✓ **Основные критерии (исходные данные)**
  - категория обрабатываемых в страховой компании ПДн
  - объем обрабатываемых в страховой компании ПДн
- ✓ **Дополнительные критерии (исходные данные)**
  - характеристики безопасности (конфиденциальн., целостность, доступность)
  - структура ИС страховой компании (локальные, распределенные)
  - наличие подключений к ССОП и СМОИ (Интернет, SWIFT и др.)
  - режим обработки ПДн (однопользовательские, многопользовательские)
  - режим разграничения прав доступа к ПДн
  - местонахождение ИС (в пределах РФ, частично за пределами РФ)

ЭЛВИС-ПЛЮС

Что надо знать о категории ПДн?

Установлены следующие категории ПДн

- ✓ **категория 1** - ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, *состояния здоровья*, интимной жизни;
- ✓ **категория 2** - ПД, позволяющие идентифицировать субъекта ПД и получить о нем *дополнительную информацию*, за исключением ПД, относящихся к категории 1;
- ✓ **категория 3** - ПД, позволяющие идентифицировать субъекта ПД;
- ✓ **категория 4** - обезличенные и (или) общедоступные ПД.

Пункт 6 Приказа №55/86/20

ИС, в которых обрабатываются персональные данные, касающиеся состояния здоровья относятся к 1 категории

ЭЛВИС-ПЛЮС

Важное замечание!

Закон РФ №5488-1 «Основы законодательства РФ об охране здоровья граждан»

«…Каждый пациент имеет право на сохранение личной тайны, и врач, равно как и другие лица, участвующие в оказании медицинской помощи, обязан сохранять врачебную тайну даже после смерти пациента, как и сам факт обращения за медицинской помощью. Тайна распространяется на все сведения, полученные в процессе обращения и лечения (диагноз, методы лечения, прогноз и др.) Лица, пользующиеся правом доступа к медицинской информации, обязаны сохранять в тайне все полученные о пациенте сведения…»

Защита медицинской информации является обязанностью всех кто имеет к ней доступ

ЭЛВИС-ПЛЮС

От чего зависит класс ИСПДн?

Установлены следующие классы ИСПДн

- **Класс типовых ИС определяется по таблице**

Количество субъектов ПД / Категории ПД	< 1000	От 1000 до 100 000	> 100 000
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

- **Класс специальных ИС определяется на основе модели угроз**

Чем выше категория ПДн и чем больше субъектов ПДн, тем выше класс ИСПДн и тем сложнее защита

ЭЛВИС-ПЛЮС

Что надо помнить при защите ПДн класса К1

Отличия в защите от боле низких классов ИСПДн

- ✓ **Более высокие требования к механизмам защиты ПДн**
  - Управление доступом по классу 1В (3А, 2А)
  - Применение межсетевых экранов по классу 3
  - Резервное копирование на отчуждаемые носители
  - Шифрование ПДн на носителях
  - Применение антивирусных программ-ловушек на АРМ
- ✓ **Необходимость исключения утечки ПДн за счет ПЭМИН**
  - Применение специальных защищенных средств обработки
  - Размещение ТС на максимальном удалении от КЗ
  - Размещение понижающих ТП в пределах КЗ
  - Применение фильтров в электрических цепях для развязки
  - Обеспечение электромагнитной развязки с другими цепями
  - Применение акустической защиты

Защита ИСПДн класса К1 требует значительных дополнительных капитальных вложений

ЭЛВИС-ПЛЮС

Что надо учитывать при обработке ПДн

Особенности обработки ПДн в страховых компаниях

- Основная информация в ИС – личная тайна клиента
- Деликатность взаимоотношений страховщиков и клиентов
- Жесткий временной регламент работы с информацией
- Наличие одновременно защищаемой и открытой информации
- Фрагментарность обработки и разные права доступа персонала
- Гетерогенность программной и аппаратной платформ ИС
- Мигрируемость информации между прикладными программами

Защита ПДн направлена на исключение несанкционированного доступа, при котором возможно их уничтожение, изменение, блокирование, копирование и распространение

ЭЛВИС-ПЛЮС

Риски страховщиков при обработке ПДн

Основные угрозы при нарушении правил обработки и защиты ПДн

- ✓ **Возможность материального ущерба**
  - Угроза судебных исков субъектов ПДн
  - Угроза административной ответственности
  - Угроза приостановления основной деятельности
  - Угроза потери клиентов (перехода к конкуренту)
- ✓ **Возможность репутационного ущерба**
  - Угроза публикации нарушений в отчетах регуляторов
  - Угроза публикации негативной информации в СМИ
  - Угроза распространения неблагоприятных слухов
  - Угроза формирования неблагоприятной судебной практики

Нарушение установленных правил обработки защиты ПДн влечет не только потерю репутации, но прямые материальные потери

ЭЛВИС-ПЛЮС

Риски страховщиков при обработке ПДн

Основные уязвимости, приводящие к реализации угроз

✓ Социально-правовые уязвимости

- Неправомерное распространение ПДн (иск в суд о возмещении ущерба)
- Нарушение порядка обработки ПДн (жалоба в надзорный орган)
- Конфликт, не связанный с обработкой ПДн (жалоба в надзорный орган)
- Отказ клиента в обработке своих ПДн (блокирование работы ИСПДн)
- Запрос сведений, касающихся обработки ПДн (ст.14,ФЗ-152 проблемы)

✓ Технико-правовые уязвимости

- Нарушение порядка обработки ПДн (проверка регуляторов)
- Отсутствие средств защиты ПДн (проверка регуляторов)
- Отсутствие документации по защите ПДн (проверка регуляторов)

Социальный аспект играет важную роль в устранении рисков страховых компаний при обработке ПДн, но не исключает необходимости решения технических проблем

ЭЛВИС-ПЛЮС

Как уменьшить риски при обработке ПДн?

Рекомендации по устранению угроз

- ✓ **Принять меры к снижению социального накала**
  - Построить позитивные отношения с клиентом
  - Декларировать гарантии по защите ПДн
  - Ясно разъяснять цели сбора и обработки ПДн
  - Предупреждать клиента обо всех операциях с ПДн
- ✓ **Принять меры по снижению класса защищенности ИСПДн**
  - Правильно оценить угрозы (модель) и исключить не актуальные
  - По возможности сократить количество субъектов ПДн
  - По возможности снизить категорию ПДн
- ✓ **Разделить риски с другими**
  - Операторы связи (провайдеры)
  - Зарубежные партнеры

ЭЛВИС-ПЛЮС

Как снизить категорию ПДн?

Основные методы снижения категории ПДн

✓ **Организационные методы**

- Уточнить необходимость для бизнеса имеющегося объема ПДн
- Применять кодирование диагнозов
- Применять при обработке обезличенные ПДн
- Перейти при обработке на табельные или абонентские номера
- Исключить часть ПДн из автоматизированной обработки

✓ **Технические методы**

- Разделить ИС на сегменты по функциональному признаку
- Выделить БД в отдельный сегмент системы – ЦОД
- Создать сегмент для ПДн, идентифицирующих субъекта
- Использовать технологии терминального доступа
- Разместить наиболее критичные ПДн на съемных носителях

Если стоимость реализации организационных и технических методов снижения категории ПДн ниже, чем стоимость системы защиты, то есть повод для раздумий

ЭЛВИС-ПЛЮС

Как удешевить систему защиты?

Пути минимизации затрат на защиту ПДн

- максимальное использование возможностей уже имеющихся в ИС средств защиты информации, возможностей ОС и прикладного ПО
- принятие дополнительных мер, позволяющих снизить требования к части ИСПДн или сегментам сети, где такие ИСПДн расположены
- сокращение количества АРМ, обрабатывающих ПДн, разделение функций пользователей, минимизирование одновременной обработки ПДн из разных систем
- разделение ИС межсетевыми экранами на отдельные сегменты (ИСПДн), классификация каждого сегмента и снижения требований к ним

Даже если ИСПДн имеет высокий класс, всегда остаются пути снижения затрат на защиту ПДн

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124498, Москва, Зеленоград,
проезд 4806, д.5, стр.23
тел. 276-02-11 факс 499) 731-24-03
e-mail: vsv@elvis.ru
http://www.elvis.ru