ЭЛВИС-ПЛЮС

Актуальные проблемы защиты персональных данных и пути их решений

Маноенко Игорь Владимирович

Консультант- аналитик
Компания «ЭЛВИС-ПЛЮС»

2010 год

ЭЛВИС-ПЛЮС

ВНИМАНИЕ!

Материалы, представленные в данной презентации не претендуют на полноту анализа рассматриваемых в ней проблем

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.

Перенос сроков приведения ИСПДн в соответствие с требованиями ФЗ № 152 на 1 января 2011 года, как ожидалось не решил проблем, стоящих перед Операторами ПДн

ЭЛВИС-ПЛЮС

Актуальность

Стоимость вложений в создание (приведение) ИСПДн для всех операторов ПДн является актуальной.

Рассмотрим несколько проблем, решение которых существенно влияет на стоимость создаваемых операторами ИСПДн.

ЭЛВИС-ПЛЮС

ПРОБЛЕМА 1

Проблема 1

Почему после выполнения работ по приведению ИСПДн в соответствие требованиям федерального законодательства желаемый результат не достигается?

Или как построить недорогую, но эффективную информационную систему персональных данных?

ЭЛВИС-ПЛЮС

Только факты

Анализ сложившейся практики приведения ИСПДн в соответствие с требованиями ФЗ показывает, что большинство интеграторов в ходе приведения ИСПДн в соответствие требованиям ФЗ строят или пытается строить систему защиты ПДн, которая, как правило у Заказчика уже есть. В то же время внедрение в процессы обработки ПДн организационных мер, выполнение которые, определяется требованиями ФЗ № 152, требованиями ТК, Постановления правительства № 687, не реализуется, а точнее - реализуется не в полном объеме.

ЭЛВИС-ПЛЮС

Кто прав, а кто виноват в том, что требования ФЗ к процессам обработки ПДн не выполняются?

Виноваты оба.

- Заказчик, как оператор ПДн
- Интегратор, как и исполнитель договора, в котором заявлено: - «Приведение ИСПДн Заказчика в соответствие требованиям федеральным законодательством»

То есть,

- Перед законом виноват Оператор ПДн
- Перед Оператором ПДн виноват Интегратор.

ЭЛВИС-ПЛЮС

Начнем сначала. Во-первых

Рассмотрим вопрос построения системы защиты ПДн

Если перечислить все необходимые для обеспечения безопасности Пдн средства и системы защиты, то в информационных системах большинства операторов они давно созданы и используются.

- У кого нет антивирусной защиты?
- У кого нет системы защиты сетевого периметра?
- У кого не используются средства защиты от НСД
- т .д.

Во-вторых

Что есть персональные данные?

Это один из видов конфиденциальной информации, которую мы защищали и до принятия ФЗ №152.

Практически все операторы защищают коммерческую тайну, другие виды тайн, и вопрос защиты ПДн - это лишь вопрос дополнительных организационных мер и использования сертифицированных средств защиты.

ЭЛВИС-ПЛЮС

А что нам предлагают?

Вернемся к практике. Что же мы видим.

«Нам» усиленно предлагают проекты по СОЗДАНИЮ СИСТЕМ ЗАЩИТЫ ПДн.

Целый ряд Интеграторов предлагает - даже аттестацию объектов ИСПДн, как некую панацею от всех бед.

И так подводим итог –

«Построение систем защиты персональных данных, для большинства Операторов – ЭТО ВОПРОС МОДИФИКАЦИИ РАНЕЕ СОЗДАННОЙ СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ».

ЭЛВИС-ПЛЮС

Теперь о ГЛАВНОМ

А что же, с внедрением в ИС Заказчика требований ФЗ № 152, ТК, требований Постановления правительства № 687?

Работы по приведению процессов обработки ПДн – это, прежде всего работы, порядок выполнения которых требует от Оператора принятие управленческих решений, которые ни один Интегратор за Оператора не выполнит.

А если и «возмется» за их выполнение, то цена вопроса уже не 300-500 тысяч РУБЛЕЙ.

Следствием сложившейся практики является

- Не выполнение всего комплекса работ по приведению ИС Заказчика в соответствие требованиям федерального законодательства.

ЭЛВИС-ПЛЮС

Кто виноват?

Виновного найти крайне сложно.

Интегратор свои работы в объеме ТЗ выполнил, получил деньги и ушел.

Сам Оператор в большинстве случаев самостоятельно не в состоянии привести свои процессы обработки ПДн в соответствие с требованиями федерального законодательства.

Что делать?

Пути решения

1. В организации должна быть создана рабочая группа с полномочиями в принятии управленческих решений.

2. Работы по приведению процессов обработки ПДн в соответствие с требованиями ФЗ должно выполняться проектной командой, состоящей как из специалистов Исполнителя, так и сотрудников Заказчика из состава рабочей группы.

ЭЛВИС-ПЛЮС

Особенности Российской действительности или **почему Заказчик должен выполнять работы на которые он СОБСТВЕННО нанял Исполнителя?**

Ответ можно получить – обратив внимание на стоимость работ, выполняемых Исполнителем в ходе аудита информационной системы.

Для того, чтобы определить требования к процедурам обработки ПДн необходимо как минимум провести обследование всех процедур управления предприятием, в границах объекта выполняемых работ. Стоимость таких работ (обследованием бизнес процессов) крайне высока.

Реально – в случае проведение полного аудита бизнес процессов Исполнителя, стоимость проекта возрастет в 3-5 раз и он становиться не по карману для большинства Заказчиков.

ЭЛВИС-ПЛЮС

Особенности Российской действительности или почему Заказчик должен выполнять работы на которые он нанял Исполнителя?

Следующая особенность.

– На волне актуальности выполнения требований ФЗ № 152, на российском рынке появилась масса разного рода компаний, которые до этого вообще проблемами информационной безопасности не занимались.

Но «приобрели» соответствующие лицензии и сертификаты, планируя «срубить на волне защиты ПДн».

Появление массы «крышующихся» интеграторов привело к тому, что привести ИСПДн в соответствие с требованием законодательства можно чуть ли не за 50 тыс. рублей. В таких условиях и серьезные Интеграторы вынуждены сбрасывать свои цены

– И как результат выполнять работы не в полном объеме, а лишь ровно на столько – насколько им заплатил Заказчик.

ЭЛВИС-ПЛЮС

Подводим результат

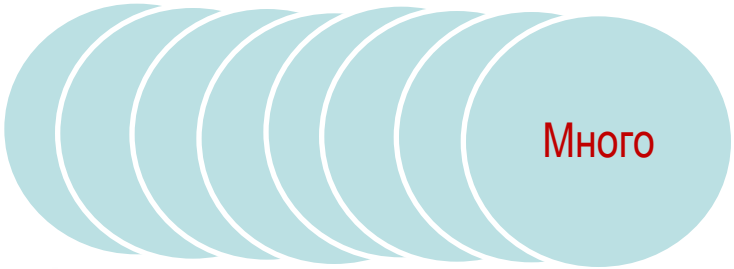
Что же делать, в сложившихся условиях

Единственно правильным на сегодняшний день решением является выполнение работ Исполнителем с привлечением со стороны Заказчика рабочей команды, имеющий опыт работы в организации и способной без серьезных трудозатрат на проведение аудита процессов обработки ПДн определить где и как выполняются данные процессы, а Исполнитель укажет для них как правильно внедрить в них требования федерального законодательства Российской Федерации.

ПРОБЛЕМА 2

Проблема 2

Как определить сколько ИСПДн в организации?



ЭЛВИС-ПЛЮС

Почему?

Вопрос 1

В информационной системе Компании есть общедоступные источники ПДн?

Ответ

Да, есть (это - корпоративные справочники, AD, почтовая система и т.д.)

В качестве вывода отметим

В информационной системе Компании есть процессы обработки ПДн, которые необходимо привести к 4 классу ИСПДн.

ЭЛВИС-ПЛЮС

Детализируем

Вопрос 2

В информационной системе Компании есть процессы, в которых ведется обработка конфиденциальных ПДн?

Ответ

Есть, во всех процессах управления персоналом, предоставления услуг клиентам Компании, в процессах взаимодействия с внешней стороной имеют место ПДн, которые привести в категорию общедоступные крайне затруднительно, а в большинстве случаях невозможно

Вывод

В информационной системе Компании есть процессы, которые необходимо привести в соответствие с 3 или 2 классом ИСПДн

ЭЛВИС-ПЛЮС

Далее

Вопрос 3

В информационной системе Компании есть электронные архивы длительного хранения со сроками хранения до 3, 5 лет?

Ответ

Есть (это архивы документов строгой отчетности: финансовой, управленческой, платежной и др. отчетности)

Вывод

В информационной системе Компании есть процессы, которые необходимо привести ко 2-му или даже к 1-му классу ИСПДн

ЭЛВИС-ПЛЮС

Обобщим выводы

В качестве общего вывода отметим:

«Для большинства операторов ПДн характерным является наличие в информационной системе Компании ПЕРСОНАЛЬНЫХ ДАННЫХ разного уровня критичности.

То есть наличие нескольких ИСПДн – для которых требования к обеспечению безопасности ПЕРСОНАЛЬНЫХ ДАННЫХ будут различны»

И так по факту - в информационной системе практически каждого оператора имеют место несколько ИСПДн с ПДн разного уровня критичности.

Например, по категориям ПДн.

ЭЛВИС-ПЛЮС

Продолжаем разговор

В условиях, когда ПДн используются практически во всех процессах управления деятельностью Компаний возникает закономерный вопрос.

Что это значит для Оператора построение нескольких систем персональных данных?

Для полноты картины ВОПРОС МОЖНО СФОРМУЛИРОВАТЬ КАК – «Построение нескольких систем управления ПРОЦЕССАМИ ДЕЯТЕЛЬНОСТИ КОМПАНИИ –

КАЖДАЯ ИЗ КОТОРЫХ - СО СВОИМИ ПРАВИЛАМИ И ПОРЯДКОМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ».

ЭЛВИС-ПЛЮС

К чему это приводит?

Во-первых, это появление сложной системы управления процессам обработки ПДн, в которой необходимо учитывать все особенности (требования) к обеспечению безопасности ПДн разного уровня критичности.

Во-вторых, это дополнительные временные, материальные и финансовые расходы на организацию и выполнение процедур контроля за выполнением процессов обработки ПДн.

И в-третьих, границы между ИСПДн разного уровня критичности настолько условны, что традиционные (организационно-технические) меры изоляции процессов обработки информации, применяемые для защиты информационных систем с разным уровнем критичности невозможно применить. Порой граница между двумя ИСПДн проходит в мозгах сотрудников Компании.

ЭЛВИС-ПЛЮС

Подводим черту

Напрашивается очередной вопрос

– А стоит ли городить огород?

Не проще ли создать единую (привести в соответствие) систему, в которой ведется обработка ПДн с разным уровнем критичности.

ЭЛВИС-ПЛЮС

Для ИСПДн без использования средств автоматизации

В случае, когда обработка ПДн ведется без использования средств автоматизации – вопрос о создании единой системы обработки ПДн вообще не стоит.

Система уже существует

Необходимо регламентировать процедуры обработки ПДн в соответствии с требованиями: ФЗ №152, ТК и Постановления правительства № 687.

ЭЛВИС-ПЛЮС

Для ИСПДн с использованием средств автоматизации

А как быть с процессами обработки ПДн в автоматизированных системах?

Обратимся к базовому документу ФСТЭК «Положение о методах и способах защиты информации в информационных системах персональных данных» и рассмотрим - насколько требования ФСТЭК для разных классов ИСПДн могут повлиять на решение о создании единой системы обработки ПДн.

ЭЛВИС-ПЛЮС

Чему нас учит ФСТЭК России?

Сравним требования к наиболее распространенным классам многопользовательских ИСПДн с разными правами доступа, а именно к 3 и 2 классам.

Требования к подсистемам: управления доступом, регистрации и учету, обеспечения целостности

Пункт 3.3. Положения ...

Для информационных систем 2 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей реализуются все методы и способы защиты информации от несанкционированного доступа, соответствующие информационным системам 3 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей.

Вывод.

Требования одинаковы. Практически такая же ситуация и при сравнении требований предъявляемых к другим классами ИСПДн.

ЭЛВИС-ПЛЮС

А что с требованиями к межсетевому взаимодействию?

А как быть с требованиями к организации межсетевого взаимодействия?

Различия в требованиях есть.

А сколько будут стоить эти различия?

Ответ на это вопрос можно найти проведя оценку возможностей средств межсетевого экранирования.

Современный парк сертифицированных межсетевых экранов обеспечивает выполнение требований для любого класса ИСПДн.

Следовательно, пытаясь оптимизировать ИСПДн, «лукавя» на понижении ее класса мы боремся с «ветряными мельницами». Ведь **стоимость необходимо оборудования, что для 1-ого, что для 2-ого, что для 3 класса одна и та же**.

ЭЛВИС-ПЛЮС

Заключение или зачем строить единую ИСПДн

Достоинства построения единой ИСПДн, состоящей из нескольких частей разного класса защищенности ПДн :

1. Стоимость создания (приведения) одной, состоящей из нескольких частей ИСПДн существенно ниже чем создание нескольких систем
2. Единая система управления, как на уровне управления процессам деятельности организации, так и на уровне процессов обеспечения технической защиты ПДн.
3. Единая система защиты ПДн, а для большинства Компаний это то вопрос внесения изменений в конфигурации уже используемых средств защиты в границах ранее построенной системы защиты коммерческой и/или банковской информации.
4. Масштабируемость системы. С увеличением количества видов деятельности организации, в которых имеют место ПДн, с единой ИСПДн уже нет необходимости строить новую ИСПДн. Необходимо лишь, определить активы с ПДн и процессы их обработки, включить их в состав уже созданной ИСПДн, регламентировав приказом по организации требования к обеспечению безопасности ПДн в соответствии с ранее установленными для той или иной части уже созданной ИСПДн.
5. Адаптивность системы. Способность быстро и своевременно реагировать на внешние и внутренние изменения в процессах обработки ПДн.
6. и т.д.

ЭЛВИС-ПЛЮС

Спасибо за внимание !

124498, Москва, Зеленоград,
проезд 4806, д.5, стр.23
тел. (495) 276-02-11, факс (499) 731-24-03
e-mail: vsv@elvis.ru
http://www.elvis.ru