



**ЭЛВИС-ПЛЮС**

# **Защита персональных данных в организациях малого и среднего бизнеса**

**(Практический опыт)**

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

**2010 год**



## **ВОПРОСЫ ПРЕЗЕНТАЦИИ**

- **Особенности SMB-сегмента**
- **Особенности IT-структуры SMB-сегмента**
- **Особенности построения защиты ПДн**
- **Примеры из жизни**



**Развитие малого и среднего предпринимательства рассматривается не только как одно из важнейших средств создания гибкого, мобильного сектора экономики с высоким потенциалом развития и самоорганизации, но и как социально и политически стабилизирующий фактор**

*О.Е. Никонова, Академия управления «ТИСБИ»*

***Сегмент SMB из-за кризиса сдал позиции – количество предприятий и их оборот заметно уменьшились. По данным Росстата на 2009 год в РФ зарегистрировано 1 млн. 348 тыс. малых предприятий. Общий годовой оборот SMB-сегмента составляет 18 трлн. 685 млрд. рублей***

## **ЧЕМ ЗАНЯТ МАЛЫЙ БИЗНЕС**

Основной спектр деятельности компаний SMB-сегмента

- **Муниципальные учреждения**
- **Медицина и рекреация**
- **ЖКХ и бытовое обслуживание**
- **Образование и юридические услуги**
- **Почтовые рассылки и электронная коммерция**
- **Строительство и недвижимость**
- **Автосервис и автотрейдинг**
- **Инвестиции и финансы**
- **Консалтинг и аудит**
- **Издательство и печать**

***SMB-предприятия в основном работают в сфере обслуживания населения, поэтому их деятельность постоянно связана с обработкой персональных данных клиентов***



## **ХАРАКТЕРНЫЕ ЧЕРТЫ БИЗНЕСА**

Что надо учитывать при работе в SMB-сегменте

- Дефицит финансовых средств и, особенно IT-бюджетов
- Отсутствие штатных специалистов по ИБ и ИТ
- Малый размер информационных систем
- Ограниченный состав необходимых прикладных систем
- Ориентирование на применение «коробочных» IT-решений
- Широкое использование Интернета и открытых сетей
- Осторожность к решениям, отдача от которых не очевидна
- Настороженность со стороны крупных IT-интеграторов
- Необходимость полноценного обеспечения защиты ПДн

***SMB отличается крупного бизнеса тем, что у этих компаний зачастую нет ни IT-департаментов, ни выделенного штатного сотрудника, занимающегося ИБ***

## **ХАРАКТЕРНЫЕ ЧЕРТЫ ИС**

Типовой портрет ИСПДн предприятия SMB-сегмента

### **✓ Используемые типовые прикладные системы**

- Бухгалтерский учет и расчет заработной платы
- Кадровый учет и медицинское страхование
- Базы данных о клиентах по профилю SMB-компании

### **✓ Характеристика типовой ИСПДн**

- количество рабочих станций – от 1 до 10 единиц
- количество серверов – от 1 до 2 единиц
- количество субъектов ПДн – от 100 до 1 000 (+ до 50 000 клиентов)
- режим обработки – многопользовательский с разными правами
- тип ПДн – идентификационные и дополнительные сведения
- выход в ССОП и Интернет – имеется
- взаимодействие с другими ИС – имеется, в т.ч. удаленные АРМ
- уже используемые средства защиты – AVP, МЭ

***Несмотря на малые размеры ИС, категория обрабатываемых ПДн может быть достаточно высокой***



**ВАЖНОЕ ЗАМЕЧАНИЕ!**

**Субъекта персональных данных не интересует крупное или малое предприятие занято обработкой его данных. При противоправных действиях с такой информацией и в том, и в другом случае ему может быть причинен ущерб.**

**Да и Закон ориентируется на защиту интересов субъекта, а не на размер бизнеса оператора ПДн.**

***Защита ПДн, независимо от размера бизнеса оператора ПДн, должна быть адекватна имеющимся угрозам***

## **ОСОБЕННОСТИ СИСТЕМЫ ЗАЩИТЫ ПДн**

Что хочет видеть SMB-сегмент от системы защиты ПДн

- Минимальный состав программных и аппаратных средств
- Малая трудоемкость и простота настройки средств защиты
- Легкость технического обслуживания и сопровождения
- Минимальная необходимость конфигурирования и управления
- Простота эксплуатации и незаметность для пользователя
- Дешевизна внедрения и эксплуатации

*Чем проще и дешевле система защиты ПДн, тем лучше для пользователей SMB-предприятия*

## **КАК СТРОИТЬ ЗАЩИТУ ПДн** Что предложить SMB-сегменту

### **✓ Организационный аспект**

- Экспресс-аудит ИС
- Консультационная поддержка организации защиты
- Разработка организационных документов по защите ПДн
- Оценка соответствия ИСПДн (декларация, аттестация)

### **✓ Технический аспект**

- Сегментирование ИСПДн и снижение класса отдельных сегментов
- Использование механизмов защиты ОС и СУБД
- Переход на технологии терминального доступа (Citrix, RDP, Sun Ray)
- Переход на Web-технологии (тонкий клиент)

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

## **КАК СТРОИТЬ ЗАЩИТУ ПДн** Терминальный доступ

### ✓ Особенности терминального доступа

- обмен с сервером только кодами клавиш и «снимками» экранов
- данные не обрабатываются и не хранятся
- изоляция терминальных сессии по данным

### ✓ Снижение требований к рабочему месту

- простая модель угроз ПДн
- ПДн не обрабатываются и не хранятся
- невозможность передать на сервер (в ЦОД) вредоносный код
- параллельная работа с открытыми и конфиденциальными данными
- из функции ИБ – защита канала и защита от клавиатурных шпионов

### ✓ Экономия на защите ИСПДн

- снижение стоимости аудита
- только защита канала и целостности (защита от сниффинга клавиатуры)
- экономия на СЗИ, AVP, IPS
- снижение стоимости аттестации

***ИСПДн с архитектурой терминального доступа – реально снижает затраты на защиту ПДн***

## КАК СТРОИТЬ СИСТЕМУ ЗАЩИТЫ ПДн

Пример: применение терминального доступа для SMB-сегмента



**Внутри тонкого клиента обработка персональных данных не ведется!**

## КАКОЕ РЕШЕНИЕ ВЫБРАТЬ?

Сравнение различных решений терминального доступа

СОСТАВ ПО И ОБОРУДОВАНИЯ	Цена АРМ на базе		
	ПК (клиент-серверная схема Microsoft)	тонкого клиента (терминал на базе Microsoft)	тонкого клиента (терминал на базе СПО Linux)
Компьютер	8 000 руб.	8 000 руб.	8 000 руб.
ОС (Windows или Linux)	5 600 руб.	2 500 руб.	300 руб.
Лицензия на доступ к серверу	900 руб.	900 руб.	Не требуется
Лицензия на терминальный доступ	Не требуется	2 700 руб.	Не требуется
AVP (ПО «Антивирус Касперского®»)	1 200 руб.	1 200 руб.	Не требуется
VPN-агент (ПО «ЗАСТАВА®-Клиент»)	2 808 руб.	2 808 руб.	2 808 руб.
СКЗИ (ПО «КриптоПРО CSP»)	1 800 руб.	1 800 руб.	1 800 руб.
Идентификатор (Смарт-карта + считыватель)	1 000 руб.	1 000	1 000 руб.
СЗИ от НСД (ПО «Аккорд-АМД3» ver.5.5)	11 400 руб.	Не требуется	Не требуется
ПО «Data Protection Manager 2007»	900 руб.	Не требуется	Не требуется
ПО «Operation Manager 2007»	950 руб.	950 руб.	Не требуется
<b>ИТОГО за 1 АРМ</b>	<b>34 558 руб.</b>	<b>21 858 руб.</b>	<b>13 908 руб.</b>

## **МИНИМУМ МИНИМОРОМ**

Что предложить совсем уж малому бизнесу

### ✓ **Техническое решение**

НАЗНАЧЕНИЕ (решаемые функции)	ТИП ОБОРУДОВАНИЯ	ЦЕНА
Управление доступом, регистрация, учет, целостность	СЗИ «ПАНЦИРЬ-С»	4 000 руб.
Предотвращение НСД к ПДн из ССОП и Интернет	МЭ «ЗАСТАВА-КЛИЕНТ»	2 150 руб.
Антивирусная защита	Dr. WEB 4,4	825 руб.
Анализ защищенности, контроль эффективности СЗИ	«ФИКС»	2 500 руб.
Обнаружение вторжений сигнатурными методами	«Snort»	Бесплатно
<b>ИТОГО</b>		<b>9 475 руб.</b>

### ✓ **Аутсорсинг**

- Управление СЗИ
- Техническое обслуживание
- Анализ защищенности

**Остальные требования надо решать организационно**

# **Спасибо за внимание !**

---

**124460, МОСКВА, Зеленоград,  
Центральный проспект, 11  
тел. 777-42-92, факс 531-8863  
e-mail: [vsv@elvis.ru](mailto:vsv@elvis.ru)  
<http://www.elvis.ru>**