Актуальность выполнения требований ФЗ 152 «О защите персональных данных» в информационных системах ВУЗов

VP GROUP

Необходимость повышения внимания к вопросам выполнения требований законодательства о защите персональных данных (ПДн)

Рост внимания к выполнению требований законодательства по защите ПДн в ИС ВУЗов

в 2010 году

Приближение определенных законом сроков подготовки ИС операторов ПДн (01.01.2011 г.)

Рост активности надзорных органов по контролю соблюдения требований законодательства

VP GROUP

Активность регуляторов в 2010 году

2010 г

Роскомнадзор запланировал проверить на предмет обработки ПДн
68 образовательных учреждений

2009 г

Роскомнадзор в отношении операторов, осуществляющих обработку ПДн, провел **432** проверки
(284-плановые / в 2010 г - 1244) ; 148-внеплановых)

В связи с нарушениями операторами требований ФЗ «О персональных данных» в Роскомнадзор поступило
465 обращений

Причины:
- отсутствие согласия на обработку ПДн;
- незаконная передача ПДн третьим лицам;
- несоблюдение условий конфиденциальности (опубликование в СМИ, размещение в общественных местах, на интернет-сайтах информации, содержащей ПДн)

VP GROUP

Источники: Роскомнадзор Публичный доклад 2009 год, Планы проверок на 2010 год

Подготовка ИС ВУЗа в рамках мероприятий по выполнению требований законодательства

- **Получение письменного согласия субъектов** на обработку (с указанием какая информация, с какой целью, в какие сроки обрабатывается и кому передается
- **Пересмотр договоров** с субъектами (работники, партнеры, клиенты)
- **Формирование документов** по порядку обработки ПДн
- **Формирование списка допущенных лиц**, ознакомление под подпись, с указанием, к какой информации допущен и в какой срок
- **Формирование списка лиц,** ответственных за защиту ПДн и их обучение
- **Формирование модели угроз**
- **Классификация ИС ПДн.** Если есть подсистемы – по наибольшей категории.
- **Уведомление** уполномоченного органа (Роскомнадзор) о намерении обрабатывать ПДн
- **Получение лицензии ФСТЭК** на осуществление деятельности по технической защите конфиденциальной информации (для ИС ПДн 1 и 2 классов)
- **Приведение защиты ПДн** в соответствие с требованиями ФЗ 152 2006 года (в т.ч. и в ИС ВУЗа)
- **Проведение аттестации/декларирование соответствия СЗИ** ИС ПДн (аттестация обязательна для ИС ПДн 1 и 2 классов)
- **Организация эксплуатации ИС ПДн** и контроля безопасности

VP GROUP

Проблемы, связанные с уведомлением об обработке персональных данных - 1

Низкая активность по уведомлению об обработке ПДн

В Реестре операторов персональных данных зарегистрировано московских университетов - 9, московских институтов - 3, московских академий – 2

(из 276 государственных и негосударственных учреждений высшего проф образования, зарегистрированных в Москве по данным МинОбразНауки за 2008 год)

Всего зарегистрировано 101 333 операторов персональных данных

Возможные ошибки в уведомлении об обработке ПДн

Уведомление не требуется, если персональные данные:

- относятся к субъектам ПДн, которых связывают с оператором трудовые отношения;
- относятся к субъектам ПДн, с которыми оператора связывают договорные отношения;
- являются общедоступными ПДн;
- включают в себя только фамилии, имена и отчества субъектов персональных данных;

VP GROUP

Источники: Роскомнадзор Реестр операторов персональных данных по состоянию на 06.05.2010

Проблемы, связанные с уведомлением об обработке персональных данных - 2

Низкая активность по уведомлению об обработке ПДн

Типичные нарушения операторов ПДн (по отчету Роскомнадзора):

• *Несоответствие сведений, указанных в уведомлении об обработке персональных данных, фактической деятельности;*

• Обработка персональных данных без согласия субъектов персональных данных.

Возможные ошибки в уведомлении об обработке ПДн

•Не заявляют об обработке ряда ПДн (успеваемость; доходы; семейное положение; социальное положение; образование; профессия)

•Заявляют не все категории субъектов, ПДн которых обрабатываются (абитуриенты)

VP GROUP

Источники: Роскомнадзор Реестр операторов персональных данных по состоянию на 06.05.2010, Роскомнадзор Публичный доклад 2009 год

Защита персональных данных в ИС ВУЗов

Факторы, влияющие на уровень требований по защите ПДн в ИС

Архитектура и масштаб ИС ПДн

- Отсутствие единого подхода к построению ИС ПДн

  Распространенной ситуацией является использование территориально удаленными факультетами или филиалами ВУЗа различного ПО для автоматизированной обработки ПДн.

Применяемые средства защиты информации

- Локальные или распределенные ИС ВУЗов
- ИС ВУЗов имеют подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

Категория и объем ПДн

- Многопользовательские ИС
- ИС с разграничением доступа

VP GROUP

Защита персональных данных в ИС ВУЗов

Факторы, влияющие на уровень требований по защите ПДн в ИС

Архитектура и масштаб ИС ПДн

Применяемые средства защиты информации

Категория и объем ПДн

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам
- использование средств антивирусной защиты
- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы
- использование защищенных каналов связи (обычно, на базе использования HTTPS)

VP GROUP

Защита персональных данных в ИС ВУЗов

Факторы, влияющие на уровень требований по защите ПДн в ИС

Архитектура и масштаб ИС ПДн

Применяемые средства защиты информации

Категория и объем ПДн

- До 2 категории

ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни

- Типичный случай - от 1тыс. до 100тыс. субъектов ПДн

VP GROUP

Защита персональных данных в ИС ВУЗов

Факторы, влияющие на уровень требований по защите ПДн в ИС

ИС	Данные	Категория	Класс ИСПДн
Системы дистанционного обучения (СДО)	Сведения о студентах, необходимые для индивидуального планирования обучения и контроля успеваемости	2 или 4 (обезли-ченные)	К2/ К4
	Сведения о студентах, необходимые для расчетов за платные образовательные услуги	3	К3
	Сведения о преподавателях, формирующих ЭОРы, групповые и индивидуальные обучающие курсы	3 или 4 (обезли-ченные)	К3/К4
Web 2.0 – online сообщества (мой круг яндекса, facebook), социальные сети (одноклассники, в контекте) и сервисы (блоги - blogs, wiki; коллажи - mash-up) для упрощения создания, обмена информацией между пользователями и совместной работы (collaboration)	Сведения о студентах, ППС, научных и инженерных работниках, необходимые для эффективного обмена знаниями (образование, опыт, интересы) и их идентификации	2 или 4 (обезли-ченные)	К2/ К4
Университетский портал и Мобильный университет	Сведения о студентах, ППС, научных и инженерных работниках, необходимые для персонализации информации (рассписание, справочники, успеваемость/посещаемость, новости, распоряжения), их идентификации для контроля доступа	2 или 4 (обезли-ченные)	К2/ К4
Электронные библиотеки, Системы управления знаниями	Сведения о студентах, ППС, научных и инженерных работниках, необходимые для персонализации информации (новые поступления); учета компетенций в СУЗ; идентификации для контроля доступа и расчетов за пользование платными сервисами	2,3,4 (обезли-ченные)	К2/К3/К4

VP GROUP

Защита персональных данных в ИС ВУЗов

Факторы, влияющие на уровень требований по защите ПДн в ИС

ИС	Данные	Категория	Класс ИСПДн
Интегрированные системы управления деятельностью ВУЗа (АХД, управление образовательной, научной и инновационной деятельностью, стратегическое планирование и финансовый менеджмент)	Сведения о студентах, необходимые для индивидуального планирования обучения и контроля успеваемости	2	К2
	Сведения о студентах, необходимые для расчетов за платные образовательные услуги	2	К2
	Сведения о ППС, научных и инженерных работниках, необходимые для кадрового и бухгалтерского учета	2	К2

Подготовка к проведению мероприятий по приведению ИС ПДн к требованиям регуляторов

- ✓снижения требований регуляторов по защите ПДн в отдельных ИС
- ✓предотвращение снижения возможностей ИС e-learning

Локализация ИС обработки персональных данных ВУЗа

Реорганизация обработки ПДн в ИС ВУЗа

Координация реорганизации всех ИС ВУЗа

планирование переноса функций анализа и подготовки отчетности

Методы реорганизации в отдельных ИС

Обезличивание ПДн

Отключение ИС от сетей общего пользования

Сегментирование и реорганизация информационного обмена между ИС

VP GROUP

Мероприятия по приведению ИС ПДн в соответствие требованиям регуляторов

VP GROUP

Изменения требований регуляторов в 2010 г.

ФСТЭК

- Введение с 15.03.2010 Положения о методах и способах защиты информации в информационных системах персональных данных (приказ ФСТЭК России от 5 февраля 2010 г. № 58)

- Отмена с 15.03.2010 документов «Основные мероприятия…» и «Рекомендации по обеспечению безопасности …» (решение от 5 марта 2010 г. ФСТЭК России)

ФСБ

Роскомнадзор

Введен в действие «Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» (зарегистрирован МинЮсте РФ 28.01.2010 года)

VP GROUP

Изменения требований регуляторов в 2010 г.

ФСТЭК

ФСБ

Роскомнадзор

В 8-ом центре ФСБ РФ проходит экспертизу проект документа, в котором более детально расписаны обновленные требования по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИС ПДн.

Данный документ будет содержать требования к обоснованию необходимости использования СКЗИ, этапам работ, правилам формирования моделей угроз, контролю установки СКЗИ и др.

(выступление представителя ФСБ РФ Тачкова Ю.В. В рамках круглого стола по теме «Защита персональных данных на финансовом и пенсионном рынке» 6-7 апреля 2010 года в Учебно-методическом информационном центре НАПФ)

VP GROUP

Изменения требований ФСТЭК в 2010 г.

Предоставлено право для обеспечения защиты операторы ИС ПДн привлекать специализированные организации, имеющие лицензию на осуществление деятельности по ТЗКИ

Исключено в явном виде требование о необходимости получения лицензии на осуществление деятельности по ТЗКИ операторами ИС ПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИС ПДн 1, 2 классов и распределенных информационных систем 3 класса

Уточнено, что выбор методов и способов защиты информации зависит от определяемых оператором угроз безопасности персональных данных (модели угроз) и от класса применяемой ИС ПДн

Уточнены требования к методам и способам защиты информации в ИС ПДн

Направления конкретизации требований к методам и способам защиты информации в ИС ПДн

- Конкретизированы методы и способы защиты при взаимодействии ИС с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования)
- Конкретизированы методы и способы защиты информации от НСД при организации удаленного доступа к ИС через сети связи общего пользования
- Упрощены требования к антивирусной защите
- Конкретизированы требования контроля отсутствия недекларируемых возможностей
- Конкретизированы требования по защите от утечек по техническим каналам
- Конкретизированы случаи применения средств (систем) анализа защищенности и обнаружения вторжений
- Обеспечена прозрачная преемственность требований по защите с повышением класса ИС

Выводы

Проведение мероприятий по защите ПДн в ВУЗе актуально и реально (с учетом упрощений законодательства)

Проведение мероприятий по защите ПДн в ВУЗе требует комплексного подхода к построению СЗИ не только в рамках одной ИС (например, СДО)

Проведение мероприятий по защите ПДн в ВУЗе является коллективной деятельностью различных специалистов ВУЗа (ИТ-специалистов, юристов, экономистов)

Наши контакты

Мы всегда рады контактам с вами и нацелены на эффективное решение поставленных задач

Группа компаний VP GROUP

Адрес: 109028, Россия,

г. Москва, Подкопаевский пер, д. 7, стр. 2

Тел./Факс.: +7 (495) 968-7070

http://vpgroup.ru/

VP GROUP