Эшелон
комплексная безопасность

Защита персональных данных в системах дистанционного/очного обучения

Дмитрий Олегович Левиев
Директор Департамента Проектов
ЗАО «НПО «Эшелон»

eLearnExpo Moscow
Москва, 9-10 июня, 2009 г.

Нормативно-законодательная база защиты персональных данных в РФ

- Конституция РФ
- Федеральный закон «О ратификации конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных» №160-ФЗ
- Конвенция совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, подписанную от имени Российской Федерации в городе Страсбурге 7 ноября 2001 года

Нормативно-законодательная база защиты персональных данных в РФ

- Федеральный закон «О персональных данных» №152-ФЗ
- Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ
- Федеральный закон «О лицензировании отдельных видов деятельности» № 128-ФЗ

Нормативно-законодательная база защиты персональных данных в РФ

- Постановление Правительства РФ от 15 декабря 2007 г. N 878 "О некоторых вопросах деятельности Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия" Распоряжение Правительства РФ от 06 июня 2007 г. N 353
- Постановление Правительства РФ от 02 июня 2008 года №418 об утверждении Положения "О Министерстве связи и массовых коммуникаций Российской Федерации"
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (постановление правительства №781 от 17.11.2007)
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (Постановление Правительства РФ от 15.09.2008 N 687)
- Порядок проведения классификации информационных систем персональных данных (приказ от 13.02.2008 №55/86/20 ФСТЭК/ФСБ/МИТС РФ)

Нормативно-законодательная база защиты персональных данных в РФ

- Регуляторы защиты персональных данных
  - ФСБ РФ
  - ФСТЭК РФ
  - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
  - Минкомсвязь России
  - Трудовая инспекция
- Уведомление уполномоченного органа
  - Не нужно для обработки данных договора с физическим лицом
  - В целях защиты жизни и здоровья физического лица

Нормативно-законодательная база защиты персональных данных в РФ

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

Нормативно-законодательная база защиты персональных данных в РФ

- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (утверждены 15 февраля 2008г. заместителем директора ФСТЭК России)
- «Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России)

Нормативно-законодательная база защиты персональных данных в РФ

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

Категорирование информации

- Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни
- Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни
- Персональные данные, позволяющие идентифицировать субъекта персональных данных
- Обезличенные и/или общедоступные персональные данные

Обоснование необходимости обработки информации

- Компания обязана обрабатывать персональные данные для выполнения условий трудового или учебного договора с физическими лицами
- Учебный центр обрабатывает персональные данные согласно учебного договора с организациями
- Компания обрабатывает персональные данные, указанные в резюме кандидатов на вакансии
- Компания обрабатывает персональные данные о членах семьи или родственниках для выполнения требований по защите информации принятой в компании или стандартом организации

Документальное представление информационных потоков

- Документооборот, включая конфиденциальный
- Взаимодействие автоматизированных систем (кадровая система, система контроля доступа, система дистанционного обучения, бухгалтерия, банк-клиент зарплатного проекта и т.д.)
- Взаимодействие персонала Компании с автоматизированными системами
- Взаимодействие Компании со слушателями и контрагентами – Заказчиками
- Оперативное хранение информации
- Архивное хранение информации

Разработка модели угроз

- На основании документа «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России) с использованием «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России) разрабатывается частная модель угроз информационной системы обработки персональных данных

Классификация системы

- Классификация информационной системы обработки персональных данных для типовых систем проводиться на основании категории информации и количества обрабатываемых одновременно данных субъектов персональных данных
- Классификация специального типа информационной системы обработки персональных данных осуществляется на основании частной модели угроз, разработанной на основании методических документов ФСТЭК России и ФСБ РФ

Классификация системы

- 4 класс системы:
  - Обезличенные персональные данные при неограниченном количестве субъектов персональных данных

Классификация системы

- 3 класс системы:
  - персональные данные, позволяющие идентифицировать субъекта персональных данных и до 100000 субъектов персональных данных в системе или персональные данные субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования
  - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию и до 1000 субъектов персональных данных в системе или в пределах конкретной организации

Классификация системы

- 2 класс системы:
  - персональные данные, позволяющие идентифицировать субъекта персональных данных и более 100000 субъектов персональных данных в системе
  - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию и от 1000 до 100000 субъектов персональных данных в системе или персональные данные субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования

Классификация системы

- 1 класс системы:
  - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию и более 100000 субъектов персональных данных в системе или персональные данные субъектов персональных данных в пределах субъекта РФ
  - Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и при любом количестве субъектов персональных данных

Разработка технического задания

- Описание необходимости обработки персональных данных
- Составление краткой характеристики системы
- Формирование требований к системе в целом
- Распределение функций управления доступом к данным и их обработкой между должностными лицами
- Определение порядка изменений правил доступа к персональным данным
- Определение порядка изменений правил доступа к резервируемым информационным и аппаратным ресурсам
- Определение порядка действий должностных лиц в случае возникновения нештатных ситуаций
- Определение порядка проведения контрольных мероприятий и действий по его результатам
- Порядок согласования технического задания с регуляторами

Разработка частного задания

- Разработка частного задания проводиться на основании технического задания и утвержденной частной модели угроз информационной системы обработки персональных данных
- При разработке частного задания рассматриваются как стандартные (типовые), так вновь создаваемые средства защиты информации.
- При отсутствии типовых средств защиты информации необходимо сертифицировать существующие

Согласование модели угроз, технического задания и частного задания с ФСБ РФ и ФСТЭК России

- ФСБ РФ и ФСТЭК России имеют право менять модель угроз и класс информационной системы обработки персональных данных при проведении проверочных мероприятий оператора
- Для минимизации риска модель угроз, технического задания и частного задания при необходимости согласуется с регуляторами
- Согласование проводиться в индивидуальном порядке

Эскизный проект

- Оператор персональных данных выделяет характерные признаки и разрабатывает описание унифицированных объектов (систем).
- Для каждого унифицированного объекта (системы) на основании технического задания и частного технического задания разрабатывается эскизный проект.

Технорабочий проект

- Для каждого объекта (системы) на базе эскизного проекта разрабатывается технорабочий проект с учетом особенностей размещения, технологических и бизнес-процессов
- Сведения, изложенные в технорабочем проекте, достаточны для реализации информационной системы обработки персональных данных и системы защиты информации

Реализация технорабочего проекта

- Реализация технорабочего проекта осуществляется организациями, имеющими необходимые лицензии ФСБ РФ и ФСТЭК России на оказание услуг в области защиты информации
- При реализации технорабочего проекта должны использоваться сертифицированные средства защиты и обработки информации

Опытная эксплуатация ИСПДн объекта

- Обучение персонала, работающего с данными субъектов персональных данных;
- Обучение технического персонала, осуществляющего эксплуатацию системы;
- Обучение технического персонала, осуществляющего эксплуатацию средств защиты системы;
- Опытную эксплуатацию системы;
- Анализ результатов опытной эксплуатации системы;
- Доработку (при необходимости) программного обеспечения системы;
- Дополнительную наладку (при необходимости) технических средств системы;

Приемо-сдаточные испытания

- Испытания на соответствие техническому заданию в соответствии с программой и методикой приёмочных испытаний.
- Анализ результатов испытания автоматизированной системы.
- Устранение недостатков, выявленных при испытаниях.

Аттестация информационных систем по требованиям безопасности

- Аттестация информационных систем 1 и 2 класса обязательна
- Для информационных систем 3 класса декларация соответствия требованиям или аттестация по требованиям безопасности
- Аттестация информационных систем осуществляется уполномоченной организацией, имеющей лицензию ФСТЭК России на проведение мероприятий по аттестации
- Методика аттестации информационной системы специального типа согласуется с ФСТЭК России и ФСБ РФ

Лицензирование деятельности оператора персональных данных

- Операторы, эксплуатирующие информационные системы обработки персональных данных 1 и 2 класса и 3 класса распределенного типа, обязаны получить лицензию ФСТЭК России на «Техническую защиту конфиденциальной информации» в установленном порядке
- При эксплуатации средств криптографической защиты в информационной системе обработки персональных данных оператор обязан получить лицензии ФСБ РФ, в соответствии с выполняемыми функциями (оказание услуг по шифрованию информации, техническое обслуживание шифросредств, распространение криптографических средств)

Изменения, вносимые в деятельность Компании

- Получение лицензий ФСБ РФ и ФСТЭК России
- Регламентация бизнес-процессов обработки информации (ПП781 и ПП687)
- Документирование работы ИТ по российским требованиям (ГОСТ, ЕСПД, ЕСКД, РД)
- Обязательное использование сертифицированных средств защиты информации
- Аттестация системы или декларация соответствия

Лицензии ФСБ РФ

- «Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств», утвержденное Постановлением Правительства РФ № 957 от 29.12.2007.
- Передача надзорных функций региональным подразделениям ФСБ РФ
- Необходимость квалифицированного персонала
- Необходимость аттестации автоматизированных систем, на которых эксплуатируются СКЗИ
- Возможна передача работ на аутсорсинг лицензиату ФСБ

Лицензия ФСТЭК России

- «Положение о лицензировании деятельности по технической защите конфиденциальной информации», утвержденное Постановлением Правительства РФ № 504 от 15.08.2006.
- Руководящие документы по защите информации
- Аттестованные автоматизированные системы и защищаемое помещение для обработки конфиденциальной информации

Регламентация бизнес-процессов

- Описание порядка обработки информации с использованием и без использования автоматизированных систем
- Документально оформленное разграничение прав доступа к информации
- Создание постоянно действующей системы управления информационной безопасностью в соответствии с требованиями руководящих документов ФСБ и ФСТЭК с учетом требований отраслевых стандартов

Документирование автоматизированных систем

- Получение от поставщика решения (программного обеспечения) эксплуатационно-технической документации согласно ЕСКД, ЕСПД или РД 50-34.698-90
- Для собственных разработок - формирование полного комплекта документации согласно ЕСКД, ЕСПД и РД 50-34.698-90
- Ведение паспортов и формуляров АС и АРМ
- Ведение формуляров средств защиты информации, в том числе средств криптографической защиты информации

Спасибо за внимание

Левиев Дмитрий Олегович
Директор Департамента Проектов
ЗАО «НПО «ЭШЕЛОН»

Тел./факс : +7 (495) 645-3809
+7 (495) 645-3810
E-mail: d.leviev@npo-echelon.ru
Сайт: http://www.npo-echelon.ru