Информационная безопасность при работе с персональными данными в учреждениях образования

Жилкин Николай,
начальник отдела по защите информации
Компания «Конус»

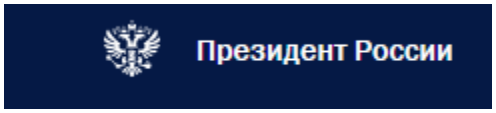
Компания «Конус»

Опыт работы в сфере защиты информации - **с 2003 года**.

Выполненные проекты :

- Подключение ВУЗов и СУЗов к ФИС ЕГЭ;
- Подключение диссертационных советов к ЕИС ГА;
- Подключение к МИС;
- Подключение защищённых рабочих мест к Региональному сегменту ГИС «Контингент» Республики Бурятия;
- Защита информационных систем в сфере социальной защиты населения;
- Разработка и внедрение системы защиты персональных данных в медицинских информационных системах;
- И многое другое.

Законы, постановления



- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»;

Законы, постановления

- Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Рекомендованные требования к минимальной функциональности средств защиты информации рабочих мест пользователей, осуществляющих информационное взаимодействие с региональной информационной системой «Контингент обучающихся» субъекта РФ.

ФЗ-152 «О персональных данных»

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку **персональных данных**, а также определяющие цели и содержание обработки **персональных данных**.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Требования ФЗ-152

Оператор при обработке персональных данных *обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных* от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. (ч.1 ст.19 ФЗ-152) .

Требования ФЗ-152

Обеспечение безопасности ПДн достигается, в частности (ч.2 ст.19 ФЗ-152):

1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
2. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
5. учетом машинных носителей персональных данных;
6. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
7. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
9. контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Определение уровня защищенности персональных данных (ПП РФ от 01.11.2012 № 1119)

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				

Приказ ФСТЭК России №17 от 11.02.2013

Государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

Муниципальные информационные системы - созданные на основании решения органа местного самоуправления.

Приказ ФСТЭК России №17 от 11.02.2013

Особенности:

- Необходимость использования сертифицированных СЗИ;
- Необходимость аттестации ГИС;
- Защита ПДн при их обработке в ГИС;
- Привлечение организаций, имеющих лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Штрафы в области защиты персональных данных

Основание	Размер штрафа		
	Физ. лица	Должностные лица	Юр. лица
Обработка ПДн в случаях, не предусмотренных законодательством РФ; обработка ПДн, несовместимая с целями сбора ПДн	предупреждение или штраф — от 1000 до 3000 руб.	предупреждение или штраф — от 5000 до 10 000 руб.	предупреждение или штраф — от 30 000 до 50 000 руб.
Обработка ПДн без письменного согласия на то их субъекта	от 3000 до 5000 руб.	от 10 000 до 20 000 руб.	от 15 000 до 75 000 руб.
Невыполнение обязанности по опубликованию или обеспечению доступа к документу, определяющему политику по обработке ПДн, или сведениям по защите ПДн	от 700 до 1500 руб.	от 3000 до 6000 руб.	от 15 000 до 30 000 руб.

Штрафы в области защиты персональных данных

Основание	Размер штрафа		
	Физ. лица	Должностные лица	Юр. лица
Непредставление субъекту ПДн информации по их обработке	предупреждение или штраф — от 1000 до 2000 руб.	предупреждение или штраф — от 4000 до 6000 руб.	предупреждение или штраф — от 20 000 до 40 000 руб.
Невыполнение оператором требования субъекта ПДн или его представителя об уточнении, блокировке, уничтожении (если ПДн неполные, устаревшие, неточные, незаконно получены, не являются необходимыми для заявленной цели обработки)	предупреждение или наложение штрафа в размере от 1000 до 2000 руб.	предупреждение или штраф — от 4000 до	предупреждение или штраф — от 25 000 до 45 000 руб.

Штрафы в области защиты персональных данных

Основание	Размер штрафа		
	Физ. лица	Должностные лица	Юр. лица
Необеспечение оператором при обработке ПДн без средств автоматизации обязанности по сохранности ПДн, что привело к неправомерному или случайному доступу к ПДн и стало причиной их уничтожения, изменения, блокирования, копирования	от 700 до 2000 руб.	от 4000 до 10 000 руб.	от 25 000 до 50 000 руб.

ГИС «Контингент»

ГИС «Контингент». Структура

Система состоит из следующих компонентов:

- Информационное взаимодействие ГИС «Контингент» с ИС ФОИВ и внебюджетных фондов
- Консолидация региональных данных на федеральном уровне
- Информационное взаимодействие регионального сегмента с региональными ИС

Минимально необходимый набор технических средств и организационных мер защиты информации

1. Защита канала связи:

- Средство криптографической защиты информации; (около 10 000р.)

ViPNet Client

2. Защита рабочей станции:

- Средство защиты от несанкционированного доступа; (от 3 500р.)

- Средство обнаружения вторжений. (от 700р.)

3. Средство Антивирусной Защиты:

- Сертифицированный по требованиям безопасности антивирус; (около 1000р.)

KASPERSKY
SECURITY

4. Разработка орг. Документации; (от 10 000р. За объект)

5. Внедрение СЗИ с проведением аттестационных испытаний; (от 9 000р.)

Наши вендоры

Код безопасности

Спасибо за внимание!

Жилкин Николай,

+7 (3012) 43-72-33 (доб. 106)
8 (924) 550-22-10
zhilkinnv@konus-b.ru

info@konus-b.ru
http://konus-b.ru