Электронные услуги в сфере образования. Обеспечение информационной безопасности.

Организация защиты персональных данных.


ИНФОРМАЦИЯ
Открытая информация
Информация ограниченного доступа
Конфиденциальная информация
Государственная тайна
Производственная тайна
Тайна следствия и суда
Служебная тайна
Персональные данные
Профессиональная тайна
Коммерческая тайна

Хронология

2005
- Ратификация конвенции совета Европы (160-ФЗ);

2006
- 152-ФЗ «О персональных данных»;

2007
- Постановление Правительства №781. Защита ИСПДн;

2008
- ПП №687. Неавтоматизированная обработка ПДн;
- Приказ ФСТЭК/ФСБ/Мининформсвязи. Классификация;
- Выпуск «четверокнижия» ФСТЭК (ДСП);
- Документы ФСБ по применению СКЗИ для защиты ПДн;

2010
- Рекомендации ФСТЭК ЮФО;
- Отмена 2 из 4 документов «четверокнижия»;
- 58 Приказ ФСТЭК – основной документ по защите ПДн;

2011
- Крупная поправка к 152-ФЗ (261-ФЗ);

2012
- Новые ПП («Уровни защищённости»);
- Обновление РД ФСТЭК и ФСБ.

РОСИНТЕГРАЦИЯ

ИЗМЕНЕНИЯ В ФЗ -152

- С 1 сентября 2015 года законом №242-ФЗ внесены

Дополнение статьи 18 частью 5.

- 5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, **находящихся на территории Российской Федерации**, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.

- **Дополнение части 3 статьи 22 пунктом 10.1.**
- 10.1) сведения **о месте нахождения базы данных информации**, содержащей персональные данные граждан Российской Федерации;

- **Дополнение части 3 статьи 23 пунктом 3.1.**
- 3.1) **ограничивать доступ к информации**, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации;

Приказ Роскомнадзора от 22.07.2015 N 85 «Об утверждении формы заявлений субъектов персональных данных о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных»

ПОЛЕЗНЫЕ ИНТЕРНЕТ-ССЫЛКИ

http://rkn.gov.ru/

- официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора), Представлены нормативные правовые акты, официальные документы и аналитические публикации по вопросу защиты прав граждан при обработке персональных данных

http://pd.rkn.gov.ru/

- «Портал персональных данных». На портале размещается информация по всему спектру деятельности Роскомнадзора в сфере защиты прав субъектов персональных данных.

http://ispdn.ru

- информационный Портал о защите персональных данных, представляющий «открытую площадку» для обсуждения вопросов в области защиты персональных данных, проектирования и использования информационных систем персональных данных (ИСПДн), форум специалистов по защите персональных данных

http://www.персональныеданные.дети

- - информационный проект для детей «Персональные данные» содержит информационно-аналитические материалы и справочную информацию во вопросу защиты прав граждан при обработке персональных данных

http://pd-info.ru/ -

информационный Портал о защите персональных данных по № 242-ФЗ

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн) В ОБРАЗОВАНИИ

Наименование характеристики ИСПДн	2012	2014
Категория обрабатываемых данных	3 категория	3 категория
Тип ИСПДн	типовая	типовая
Структура ИСПДн	автономная	распределенная
Класс ИСПДн	К3 (личные дела)	К2 (АИС «Сетевой город»)

ДЕЙСТВИЯ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

(примерный перечень –
ч. 1 ст. 18.1, ч. 2 ст. 19 Закона)

- Соблюсти принципы обработки персональных данных. Уничтожить ПД по достижении целей их обработки. (ст. 5 Закона)
- Предпринять предусмотренные Законом меры для обеспечения конфиденциальности полученных ПД. (ч. 1 ст. 7 Закона)
- Представлять ПД по требованию субъекта или его законного представителя, а также уполномоченного органа по защите прав субъектов ПД. (ч. 2 ст. 14; ч. 4 ст. 20 Закона)
- Получить согласие субъекта ПД на их обработку. (ч. 1 ст. 6 Закона)
  В случаях, предусмотренных Законом, оформить письменное согласие.

ДЕЙСТВИЯ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

(ЧАСТЬ 2)

- Назначить лицо, ответственное за организацию обработки ПД в организации (ст. 22.1 Закона)
- Проинформировать лиц, осуществляющих обработку персональных данных, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных НПА, а также локальными правовыми актами организации. (п. 6 Постановления № 687)
- Определить места хранения персональных данных (материальных носителей) в отношении каждой категории персональных данных. Установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. (п. 13 Постановления №687)
- Обеспечить сохранность персональных данных и исключить несанкционированный к ним доступ. Установить соответствующий перечень мер, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер. (п. 15 Постановления № 687)

ДЕЙСТВИЯ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (ПРИ НЕОБХОДИМОСТИ) (ЧАСТЬ 3)

- Уведомить по предусмотренной законом форме уполномоченный орган по защите прав субъектов ПД о намерении осуществлять обработку данных. (ч. 1 ст. 22 Закона)
- Соблюсти требования к типовым формам документов, характер информации в которых предполагает или допускает включение в них персональных данных. (п. 7 Постановления № 687)
- Необходимость ведения журнала (реестра, книги), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц, имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных.

(п. 8 Постановления № 687)

ПОРЯДОК ДЕЙСТВИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Подход к защите ПДн

Компьютер

Угроза «Кончился тонер»	Угроза «Перебои со светом»	Угроза «Вирус на флешке»
Ущерб: небольшой	Ущерб: средний	Ущерб: значительный
Вероятность: низкая	Вероятность: средняя	Вероятность: средняя
Неактуальная	Актуальная	Актуальная
Резервирование СВТ	Бесперебойное питание	Антивирусная защита

Контрмеры (согласно РД ФСТЭК и ФСБ)

РОСИНТЕГРАЦИЯ

ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ УЧРЕЖДЕНИЯ

Результатом проведения предпроектного обследования должны быть ответы на следующие вопросы:

- **Проекты, в рамках которых происходит обработка персональных данных.**
- **Перечень обрабатываемых категорий ПДн для каждого проекта (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, др.).**
- **Можно ли исключить какую-нибудь категорию ПДн из обработки?**
- **Краткое описание процесса работы с ПДн для каждого проекта. Какое программное обеспечение используется.**
- **Физическое расположение серверов, рабочих мест пользователей. ФИО и должность сотрудников, работающих с данными. Есть ли доступ в интернет с ПК этих сотрудников?**
- **Существующая технология сбора, хранения, обработки ПДн (данные обрабатываются локально на серверах, локально на рабочих местах пользователей, передача с использованием каналов передачи данных, по ЛВС и т. п.)**
- **Где хранятся документы на бумажных носителях? Имеются ли сейфы? Как происходит процедура уничтожения бумажных носителей персональных данных, цель обработки которых достигнута?**
- **Где располагается серверное помещение? Как организован туда доступ?**
- **Схема локальной сети.**

ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ УЧРЕЖДЕНИЯ

Результатом проведения предпроектного обследования должны быть ответы на следующие вопросы:

- Как организован доступ в интернет?
- Существуют ли какие-то регламенты, инструкции, положения и т. п. по осуществлению информационного обмена, обеспечению информационной безопасности, защите персональных данных?
- Наличие контролируемой зоны. Как осуществляется охрана периметра контролируемой зоны?

Контролируемая зона – охраняемая территория, в которой исключено пребывание посторонних лиц и не размещаются посторонние организации.

После сбора всех необходимых сведений можно переходить к базовым мерам по обеспечению безопасности персональных данных.

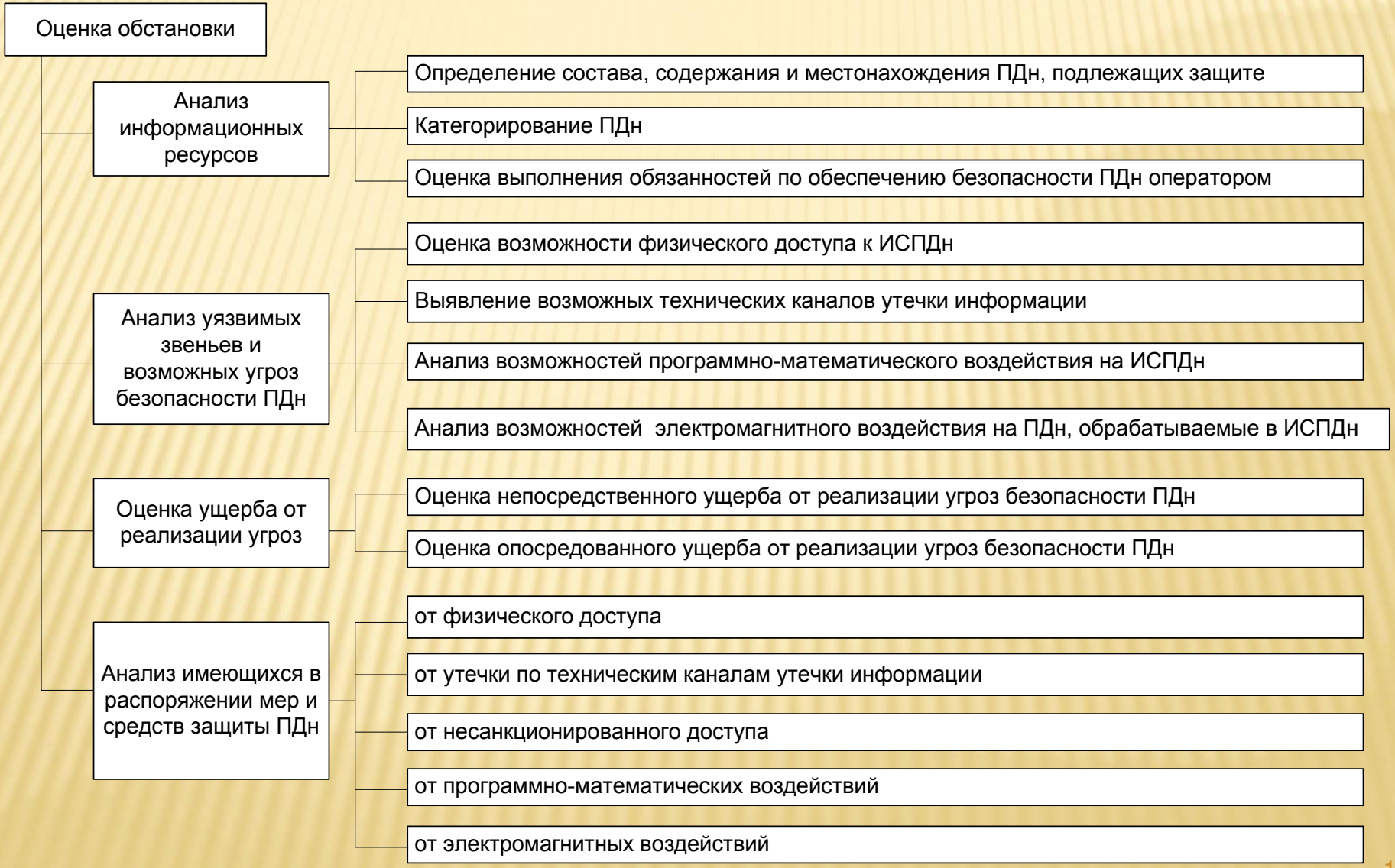
БАЗОВЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Классифицировать информационную систему персональных данных
- Подать уведомление об обработке (о намерении осуществлять обработку) персональных данных
- Получить согласие субъектов на обработку персональных данных
- Утвердить список лиц, имеющих доступ к ПДн
- Разработать журнал обращений граждан для получения доступа к персональным данным

ЭТАПЫ СОЗДАНИЯ СИСТЕМЫ ПО ЗАЩИТЕ ПДн:

- Определение мест хранения ПДн
- Организация мероприятий по защите ПДн от несанкционированного доступа
- Разработка внутренних документы по защите ПДн
- Проектировка и внедрение системы защиты ПДн
  - разработка модели угроз
  - разработка технического задания
  - приобретение технических и программных средств
- Оценка соответствия ИСПДн (Аттестация рабочего места)

ПРОЕКТИРОВКА СИСТЕМЫ ЗАЩИТЫ ПДН



МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ДАННЫХ

- Определение средств защиты ПДн от утечки по техническим каналам
- Определение средств защиты ПДн от несанкционированного доступа
- Определение средств защиты каналов при передаче ПДн

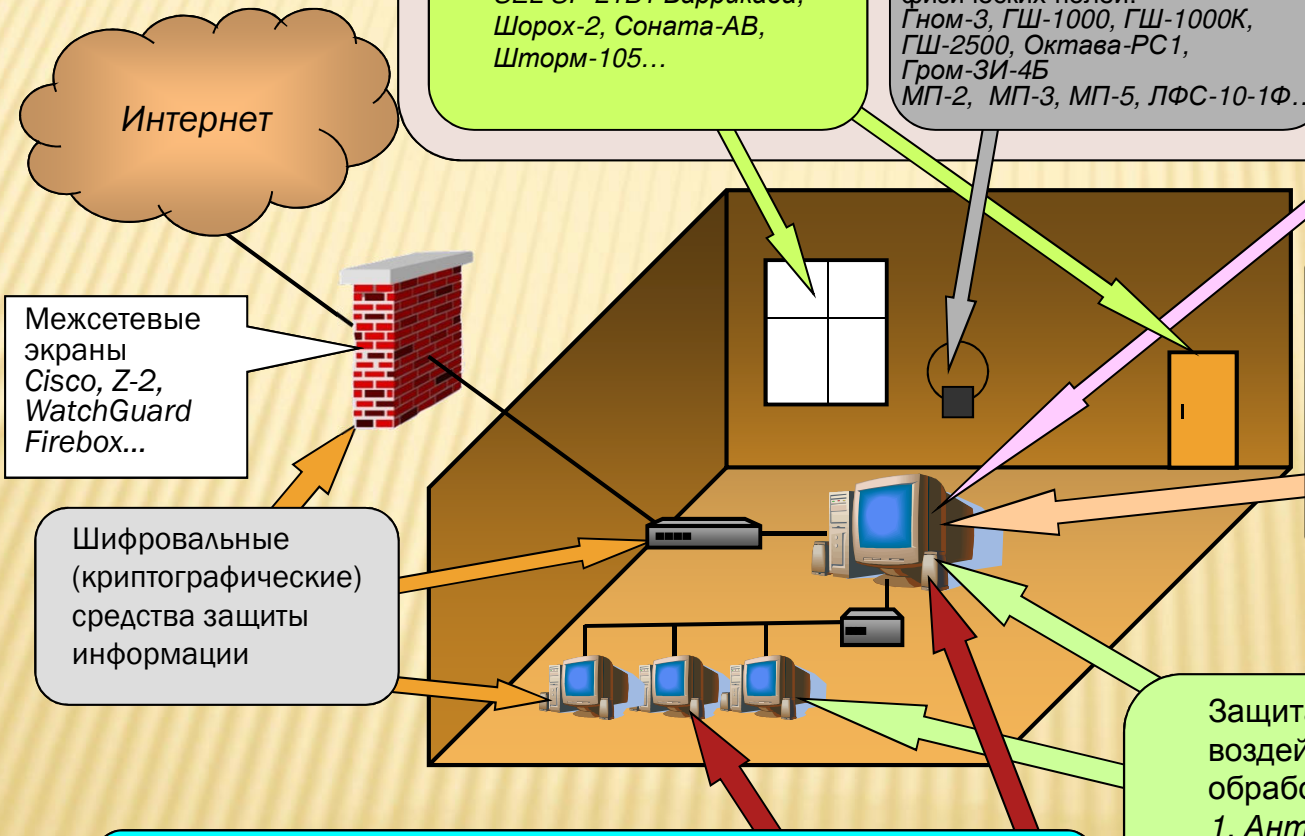
МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ДАННЫХ

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Средства защиты речевой информации:
Барон, ЛГШ-402(403), SEL SP-21B1 Баррикада, Шорох-2, Соната-АВ, Шторм-105…

Средства защиты информации, представленной в виде информативных электрических сигналов, физических полей:
Гном-3, ГШ-1000, ГШ-1000К, ГШ-2500, Октава-РС1, Гром-ЗИ-4Б МП-2, МП-3, МП-5, ЛФС-10-1Ф…

Средства защиты носителей информации на бумажной, магнитной, магнитооптической и иной основе:
eToken PRO 64K и eToken NG-OTP, Secret Disk 4…



Межсетевые экраны
Cisco, Z-2, WatchGuard Firebox…

Шифровальные (криптографические) средства защиты информации

Используемые в информационной системе информационные технологии
1. Защищенные ОС:
Red Hat Enterprise Linux, QNX, МСВС 3.0..
2. Системы обнаружения вторжений и компьютерных атак:
ФОРПОСТ, Proventia Network…
3. Шлюзы безопасности:
CSP VPN Gate, CSP RVPN…

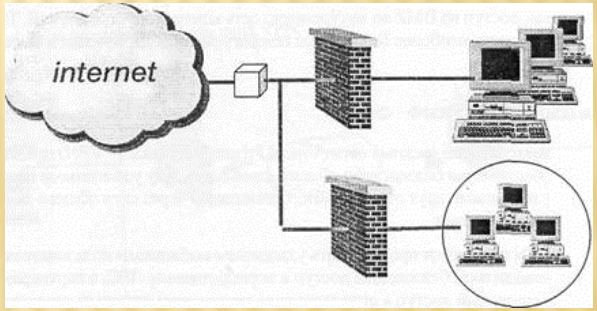
Защита от программно-технических воздействий на технические средства обработки персональных данных
1. Антивирусные средства:
DrWed, Антивирус Касперского…
*2. Программное обеспечение, сертифицированное на отсутствие НДВ **

Средства защиты информации от несанкционированного доступа:
Блокхост-сеть, Аккорд-Рубеж, Аккорд-NT/2000, Secret Net 5.0, Соболь, Dallas Lock 7.0, Лабиринт-М, Страж NT

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - МЕЖСЕТЕВОЙ ЭКРАН

Межсетевой экран - комплекс аппаратных и программных средств в компьютерной сети. Основной задачей сетевого экрана является защита сети или отдельных её узлов от несанкционированного доступа. Обеспечивают безопасность при осуществлении электронного обмена информацией **с другими системами и внешними сетями, разграничение доступа (аутентификация)** в корпоративной сети, а также защиту от проникновения и вмешательства в работу АС нарушителей из внешних систем, противодействие некоторым сетевым атакам

Брандма́уэр, файервол (Firewall)



Межсетевой экран:

- не защищает узлы сети от проникновения через уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
- не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Защита от сетевых атак, взломов – установка лицензионного программного обеспечения и проверенного на отсутствие уязвимостей и НДВ -

НЕ ДЕКЛАРИРУЕМЫХ ВОЗМОЖНОСТЕЙ

ФСТЭК

Федеральная служба по техническому и экспортному контролю

http://fstec.ru/

ОБЯЗАТЕЛЬНОСТЬ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

п.5. Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (ПП 781)

Программное обеспечение VIPNET CLIENT 3.X (КС2)

- Программное обеспечение ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях. Содержит встроенный криптопровайдер, Сертифицирован ФСТЭК.

  ViPNet Client функционирует под управлением операционных систем MS Windows: Windows XP SP3 (32-разрядная) / Windows Server 2003 (32-разрядная) / Windows Vista SP2 (32/64-разрядная) / Windows Server 2008 (32/64-разрядная) / Windows 7 (32/64-разрядная)/Windows Server 2008 R2 (64-разрядная).

- АИС «Сетевой город» объединена единой глобальной сетью **№2312** через **ViPNet**

КАК ОРГАНИЗОВАТЬ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

- обеспечить безопасность ПДн самостоятельно;
- передать обеспечение безопасности ПДн сторонней организации;
- выполнить часть работ самостоятельно, а часть доверить сторонней организации.

- Аутсо́рсинг (от англ. outsourcing: (outer-source-using) использование внешнего источника/ресурса) — передача организацией, на основании договора, определённых бизнес-процессов или производственных функций на обслуживание другой компании, специализирующейся в соответствующей области.

Аутсорсинг

- Установка и настройка СЗИ (СКЗИ)
- Контроль эффективности СЗИ, Аттестация/переаттестация
- Организационное обеспечение защиты ПДн
- Участие в проверках РКН, ФСБ, ФСТЭК
- Обучение, инструктаж, контроль знаний персонала
- Расследование инцидентов
- Защищенный документооборот. Услуги удостоверяющего центра.

РОСИНТЕГРАЦИЯ

УСЛУГИ СТОРОННИХ ОРГАНИЗАЦИЙ

Проведение работ по защите информационных систем

по требованиям ФЗ № 152 «О персональных данных».

- Аудит информационной безопасности
- Проектирование систем защиты информации
- Внедрение систем защиты информации и персональных данных
- Разработка нормативно-распорядительных документов в области защиты информации
- Оценка соответствия СЗ ИСПДн требованиям регуляторов (аттестация)
- Проведение работ по защите информации в автоматизированных системах обработки конфиденциальной информации

ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА ЗА НАРУШЕНИЕ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Административная

- Отказ в предоставлении гражданину информации (ст. 5.39 КоАП РФ)
- Нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных (ст. 13.11 КоАП РФ)
- Разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ)

Гражданско-правовая

- Ст. 17 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Уголовная

- Нарушение неприкосновенности частной жизни (ст. 137 УК РФ)
- Отказ в предоставлении Гражданину информации (ст. 140 УК РФ)
- Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

Что дешевле?

РОСИНТЕГРАЦИЯ

КАК ПОПАСТЬ ПОД ПРОВЕРКУ

1. Быть в Плане проверок РКН, ФСТЭК, ФСБ;

2. Не отреагировать на запрос РКН;

3. Нарушить права субъекта ПДн;

4. Пришла проверка к вышестоящей организации.

НАРУШЕНИЯ

В договорах с контрагентами, которым передаются ПДн, отсутствует перечень действий (операций) с ПДн, цели обработки, **обязанность соблюдения конфиденциальности**, требования к защите ПДн (часть 3 статьи 6 152-ФЗ).

Пример: «зарплатный» банк, привлечение ЧОП, корпоративный спортзал, негосударственный пенсионный фонд и т.д.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.

НАРУШЕНИЯ

Неопределённы **места хранения материальных носителей** и перечень лиц, имеющих к ним доступ. Не соблюдаются условия по обеспечению сохранности материальных носителей ПДн (п. 13 и 15 ПП687).

Пример: отсутствует утвержденный перечень мест хранения материальных носителей, перечень лиц, допущенных к обработке ПДн. Не соблюдаются правила хранения документов.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.

НАРУШЕНИЯ

Оператор до начала обработки персональных данных обязан уведомить РОСКОМНАДЗОР о своем намерении осуществлять обработку персональных данных (ч.1 ст. 22 152-ФЗ).

Пример: уведомление не отправлено, либо не актуально.

КоАП, ст. 19.7:

Непредставление или несвоевременное представление в государственный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, а равно представление в государственный орган таких сведений в неполном объёме или в искажённом виде ..

Прокуратура. Предупреждение или штраф.

НАРУШЕНИЯ

Согласие субъекта на обработку его персональных данных в случаях, когда отсутствует правовое основание (ФЗ) или с субъектом не заключен договор и т.д.

Пример: сбор сведений о близких родственниках, супругах, хранение сведений об уволенных сотрудниках и т.д.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.

НАРУШЕНИЯ

Публикация персональных данных субъекта в СМИ (и не только) без его согласия.

Пример: списки должников, победители конкурса на сайте, биография руководителя на сайте, доска почета и т.д.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.

НАРУШЕНИЯ

Персональные данные должны отвечать целям обработки. Не допускается обработка избыточных, неполных, неактуальных персональных данных (ст.5 152-фз).

Пример: «девичья фамилия бабушки», сведения о родственниках и членах семьи, адрес прописки и проживания и т.д.

КоАП, ст. 13.11:

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Прокуратура. Предупреждение или штраф.

НАРУШЕНИЯ

Лица, допущенные к ПДн, должны быть ознакомлены со всеми внутренними и внешними нормативными документами по защите ПДн под роспись (п.6 ПП687, п.8 ст. 86 ТК РФ).

Пример: Листы ознакомления с внутренними приказами, инструктаж по технике безопасности ПДн и т.д.

Особенности ведения журнала учёта посетителей (п.8 ПП687).

Требования к типовым формам (анкетам), содержащим ПДн (п.7 ПП687).

НАРУШЕНИЯ

Не назначено ответственное лицо (ст. 22.1 152-ФЗ).

Не опубликована политика обработки ПДн (п.2 ст.18.1 152-ФЗ).

(ч.1 ст. 18.1 152-ФЗ):
Не описаны технические меры по защите ПДн;
Не проводится внутренний контроль и (или) аудит соответствия;
Не оценён возможный вред субъекту.

(ч.2 ст.19 152-ФЗ)
Не принимаются технические меры по защите ПДн;
Не определены угрозы персональным данным;
Применяются не сертифицированные СЗИ;
ИСПДн не аттестована:
Не проводится контроль и оценка эффективности принимаемых мер по технической защите ПДн.

ЗАДАЧИ:

- Приобрести/продлить лицензионное ПО как мера контроля ПО за отсутствием НДВ – не декларируемых возможностей, в т.ч. уязвимостей
- Провести мониторинг безопасности ИСПДн с учетом приобретения VipNet Client

СПАСИБО ЗА ВНИМАНИЕ!