Защита персональных данных в информационных системах Администрации г. Улан-Удэ

Докладчик:
Новолодский Дмитрий Владимирович

План семинарского занятия

- Определения.
- Разъяснения по заполнению организационно-распорядительных документов по защите ПДн.
- Обязанности должностных лиц по защите информации при организации и выполнении работ по обработке ПДн и ИСПДн.
- Ведение журналов.
- Защита файлов содержащих ПДн.

- Ответы на вопросы

Определения:

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. (*Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»*).

Базой данных – является представленная в *объективной* форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)» (***Гражданский кодекс РФ, ст. 1260***).

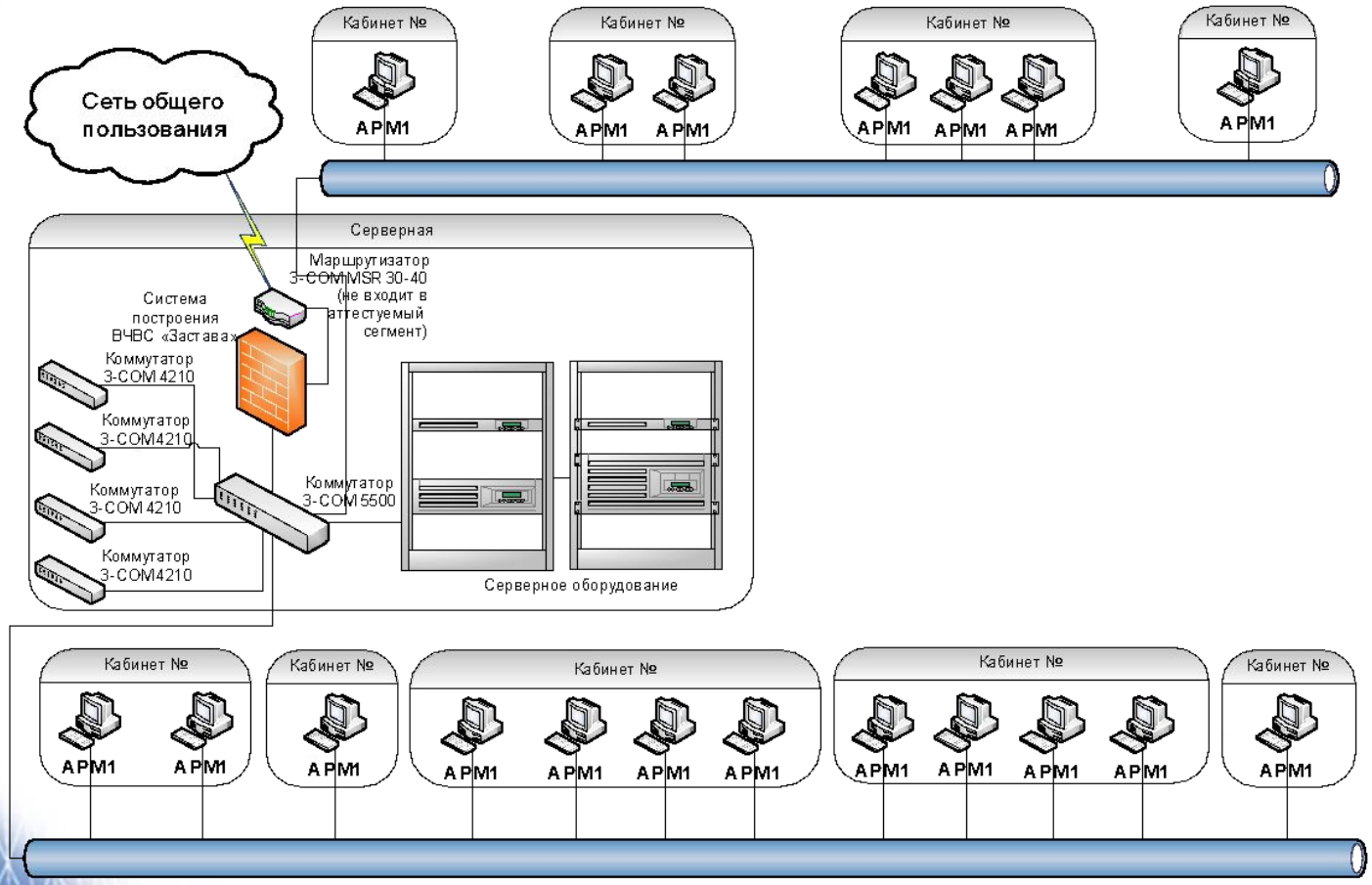
Типовая информационная система - информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

Специальная информационная система - информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

(Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»)

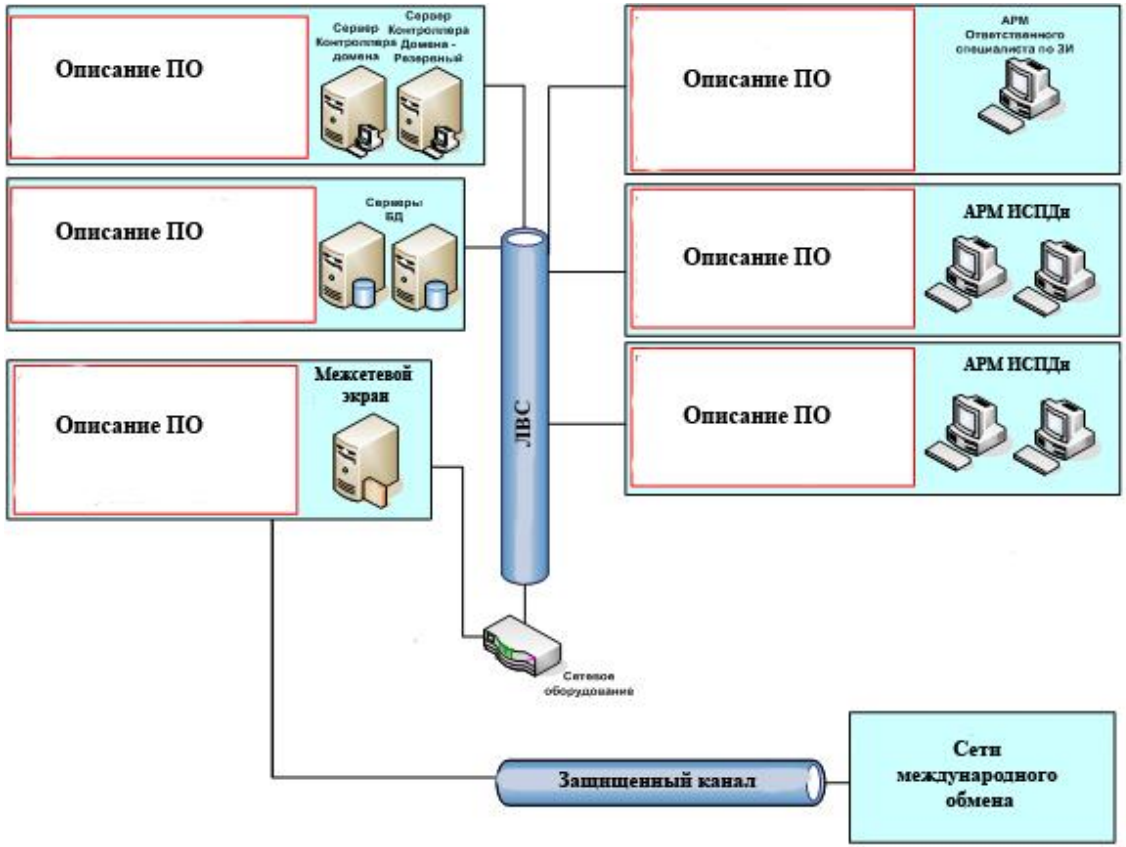
Организационные мероприятия

Схема размещения объекта информатизации относительно контролируемой зоны и линии связи



Организационные мероприятия

Структурно-функциональная схема объекта информатизации



Технический паспорт ИСПДн

СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Перечень оборудования, входящего в состав ИСПДн

№ п/п	Тип основных технических средств и систем (ОТСС)	Заводской номер	Имя ПЭВМ, место установки

СОСТАВ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Перечень средств обработки защищаемой информации, системного программного обеспечения

№ п/п	Наименование и тип технического средства	Заводской номер или номер лицензии	Сведения о сертификате	Место установки

СОСТАВ ПРОГРАММНЫХ СРЕДСТВ

Перечень используемых в ИСПДн программных средств не предназначенных для обработки защищаемой информации

№ п/п	Наименование и тип программного средства	Место установки	Комментарии

СОСТАВ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень средств защиты информации, установленных в ИСПДн

№ п/п	Наименование и тип технического средства	Заводской номер или номер лицензии	Сведения о сертификате	Место установки

СВЕДЕНИЯ ОБ АТТЕСТАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Ранее аттестация не проводилась.

Проводилась кем\дата.

ПЕРИОДИЧНОСТЬ КОНТРОЛЯ

Учет проведения периодического контроля

№ п/п	Наименование организации, проводившей проверку	Дата проведения проверки	Результаты проверки, номер отчетного документа

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Регистрация изменений

Порядковый № и дата введения изменений	Наименование документа фиксирующего изменения	№ замененных (исправленных) листов формуляра	Подпись лица, внесшего изменения

Журналы ИСПДн

ЖУРНАЛ УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ДАННЫХ

_____

(название ИСПДн)

_____

(название структурного или подведомственного подразделения)

№ п/п	Дата и время	Вид носителя	Название носителя	Учётный или серийный номер носителя	Фамилия И.О. и подпись лица, выдавшего носитель	Фамилия И.О. и подпись лица, принявшего носитель

ЖУРНАЛ УЧЕТА ПЕЧАТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

_____

(название ИСПДн)

_____

(название структурного или подведомственного подразделения)

№ п/п	Дата и время	Название документа	Учётный номер документа	Количество листов в документе	Фамилия И.О. и подпись лица, которым был напечатан документ

ЖУРНАЛ УЧЕТА ПАРОЛЕЙ

_____

(название ИСПДн)

_____

(название структурного или подведомственного подразделения)

№ п/п	Дата регист-рации	Дата удаления	Учётная запись (если есть)	Пароль	Фамилия И.О. и подпись лица, выдавшего пароль	Фамилия И.О. и подпись лица, принявшего пароль

Обязанности Ответственного по защите информации

Ответственный по защите информации обязан:

- знать перечень задач, решаемых пользователями на объекте ИСПДн, и согласно перечню защищаемых ресурсов обеспечивать их защиту.
- вводить таблицы (параметры) разграничения доступа к защищаемым ресурсам на средствах защиты информации объектов ИСПДн и своевременно их корректировать.
- подготавливать и выдавать под роспись пользователям ИСПДн личные пароли доступа (электронные ключи с записанными на них идентификационными и аутентификационными данными пользователя).
- осуществлять установку, настройку и при необходимости контроль функционирования системы защиты.
- вести архивы системных журналов с регистрационной информацией и проводить оперативный анализ этих журналов. При обнаружении предпосылок и фактов НСД к защищаемым ресурсам ИСПДн принимать меры, определенные в инструкции, докладывать начальнику.
- обеспечивать контроль работы средств защиты информации, применяемых на объектах ИСПДн, а также контроль выполнения установленного руководящими распорядительными документами комплекса организационных мероприятий по ЗИ.
- проводить тестирование средств защиты информации, осуществлять контроль их технического обслуживания.

Обязанности Ответственного по защите информации

- контролировать целостность (неизменность), сохранность средств защиты используемых в ИСПДн, а при обнаружении фактов изменения контролируемых параметров немедленно докладывать руководству.
- осуществлять постоянный контроль за соблюдением пользователями порядка печатания выходных документов, использованием средств копирования данных, антивирусной защиты, стирания информации, а также за отсутствием на АРМ пользователей средств отладки ПО.
- периодически проверять общесистемное и сетевое ПО и используемые энергонезависимые машинные носители информации всех серверов и АРМов на наличие компьютерных вирусов. В случае обнаружения вирусов или следов их воздействия немедленно докладывать об этом руководству и принимать все возможные меры к удалению их из ПЭВМ и ликвидации последствий их воздействия. Специалист по защите информации имеет право привлекать к этой работе пользователей ИСПДн.
- вести учет и обеспечивать надежное хранение используемых для функционирования средств защиты от НСД ключевых средств (ключевых носителей и сгенерированных с помощью датчиков случайных чисел паролей, носителей информации устройств блокировки и т.п.).
- осуществлять контроль защиты информации при проведении технического обслуживания и ремонта аппаратных средств ИСПДн.

Обязанности ответственного за эксплуатацию ИСПДн

Ответственный за эксплуатацию ИСПДн обязан:

- планировать мероприятия по защите информации от НСД на объектах ИСПДн, определять порядок действий сотрудников при стихийных бедствиях и при иных угрозах ИСПДн;
- устанавливать персональную ответственность должностных лиц ИСПДн, пользователей за эксплуатацию конкретных технических и программных средств, системы защиты информации от НСД на объекте, определять по согласованию с пользователями порядок формирования и использования информационного обеспечения, использования средств копирования данных, средств отладки программ и стирания информации;
- определять списки сотрудников, допускаемых в помещения ИСПДн;
- определять списки сотрудников, имеющих право вскрывать помещения ИСПДн.
- определять списки сотрудников, имеющих право доступа к обработке конфиденциальной информации.
- контролировать своевременность представления заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.
- организовывать специальную подготовку подчиненных должностных лиц по вопросам защиты информации.

Обязанности ответственного за эксплуатацию ИСПДн

- обеспечивать строгое выполнение требований по защите информации при организации проведения технического обслуживания средств вычислительной техники, вскрытии корпусов системных блоков ПЭВМ, изъятии и уничтожении конфиденциальных машинных носителей информации.
- организовывать работу по анализу возможных каналов утечки защищаемой информации на объекте ИСПДН и их закрытию.
- обеспечивать хранение средств программного и информационного обеспечения ИСПДн, конфиденциальных машинных носителей информации и выдачи носителей информации устройств блокировки.

Обязанности пользователей, осуществляющих эксплуатацию ИСПДн

1. Должностные лица, являющиеся пользователями ИСПДн, обязаны строго соблюдать установленные правила работы на комплексах средств автоматизации ИСПДн и несут персональную ответственность за неукоснительное выполнение требований и мероприятий по защите информации на своих автоматизированных рабочих местах.
2. Пользователи обязаны:
3. знать технологическую инструкцию пользователя по защите информации в ИСПДн и выполнять ее требования.
4. знать и использовать должным образом свои права по доступу к защищаемым ресурсам ИСПДн.
5. не пытаться работать от имени других пользователей.
6. знать правила работы со средствами защиты информации, порядок входа и регистрации в сети.
7. уметь пользоваться средствами антивирусной защиты и при необходимости проверять АРМ на наличие программ – «вирусов».
8. при работе на АРМ использовать только учтенные установленным порядком машинные носители информации, штатное системное и прикладное программное обеспечение.
9. знать и соблюдать правила работы с прикладным программным обеспечением.
10. не использовать выявленные слабости в защите сервисов и локальной сети в целом.
11. в случаях компрометации пароля, обнаружении фактов или предпосылок несанкционированного доступа к защищаемым ресурсам сообщать об этом ответственному специалисту по защите информации.

Ограничения, накладываемые на работу всех пользователей ИСПДн

Должностное лицо после прочтения инструкции должно расписаться в листе ознакомления.

Всем пользователям ИСПДн, запрещается:

1. проводить работы на средствах вычислительной техники без выполнения всех основных мероприятий по защите информации;
2. самовольно вносить изменения в состав, конструкцию, и размещение серверов, АРМ и коммуникационного оборудования;
3. устанавливать и использовать при работе на АРМ неразрешенное к применению программное обеспечение;
4. открывать крышки устройств и блоков технических средств ИСПДн;
5. допускать к результатам решения задач (в том числе промежуточным) лиц, не имеющих к ним прямого отношения;
6. приступать к работе на АРМ без оформления заявки и допуска установленным порядком;
7. использовать при работе на АРМ неучтенные установленным порядком машинные носители информации;
8. осуществлять выдачу конфиденциальных документов на локальный принтер без выполнения правил по защите информации;
9. приносить на службу и использовать для решения служебных задач в составе ИСПДн личные ПЭВМ и машинные носители информации;
10. производить копирование конфиденциальной информации на неучтенные машинные носители, в том числе для временного хранения информации;

Ограничения, накладываемые на работу всех пользователей ИСПДн

- уничтожать, копировать или производить какие-либо другие действия над программами (файлами), базами данных других пользователей без их разрешения;
- отключать средства специальной защиты;
- работать на средствах ИСПДн при обнаружении компьютерных вирусов или каких-либо неисправностей;
- передавать пароль или носитель информации устройства блокировки от АРМ другим лицам;
- производить подбор пароля другого пользователя;
- превышать свои полномочия при работе на АРМ;
- оставлять без присмотра ПЭВМ или АРМ до окончания сеанса работы в сети или без блокировки экрана монитора;
- осуществлять попытки входа в сеанс связи с другими информационными системами или сетями, не входящих в состав ИСПДн;
- проводить работы по исследованию обнаруженных компьютерных вирусов на технических средствах ИСПДн;
- создавать или модифицировать программы для средств вычислительной техники или вносить изменения в существующие программы, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы серверов, АРМ или сети в целом, а равно использование либо распространение таких программ или машинных носителей с такими программами.

Вопросы.

Докладчик:

Новолодский Дмитрий Владимирович