ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
современные технологии
Ижевск, 21 мая 2009

Применение решений ГК «ИНФОРМЗАЩИТА» для выполнения требований по защите персональных данных и конфиденциальной информации

Илюхин Максим

Заместитель генерального директора компании «Код Безопасности»

Законы и нормативные документы

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена

В целях обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети "Интернет", п о с т а н о в л я ю:

1. Установить, что:

а) подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети "Интернет" (далее - информационно-телекоммуникационные сети международного информационного обмена), не допускается;

б) при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных в подпункте "а" настоящего пункта, к информационно-телекоммуникационным сетям

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 17 ноября 2007 г. № 781

МОСКВА

Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии со статьей 19 Федерального закона "О персональных данных" Правительство Российской Федерации **п о с т а н о в л я е т**:

1. Утвердить прилагаемое Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Федеральной службе безопасности Российской Федерации и Федеральной службе по техническому и экспортному контролю утвердить в пределах своей компетенции в 3-месячный срок нормативные правовые акты и методические документы, необходимые для выполнения требований, предусмотренных Положением, утвержденным настоящим постановлением.

Председатель Правительства Российской Федерации В.Зубков

КОАП РФ
от 30 декабря 2001 года N 195-ФЗ

Статья 13.11.
Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Статья 13.13.

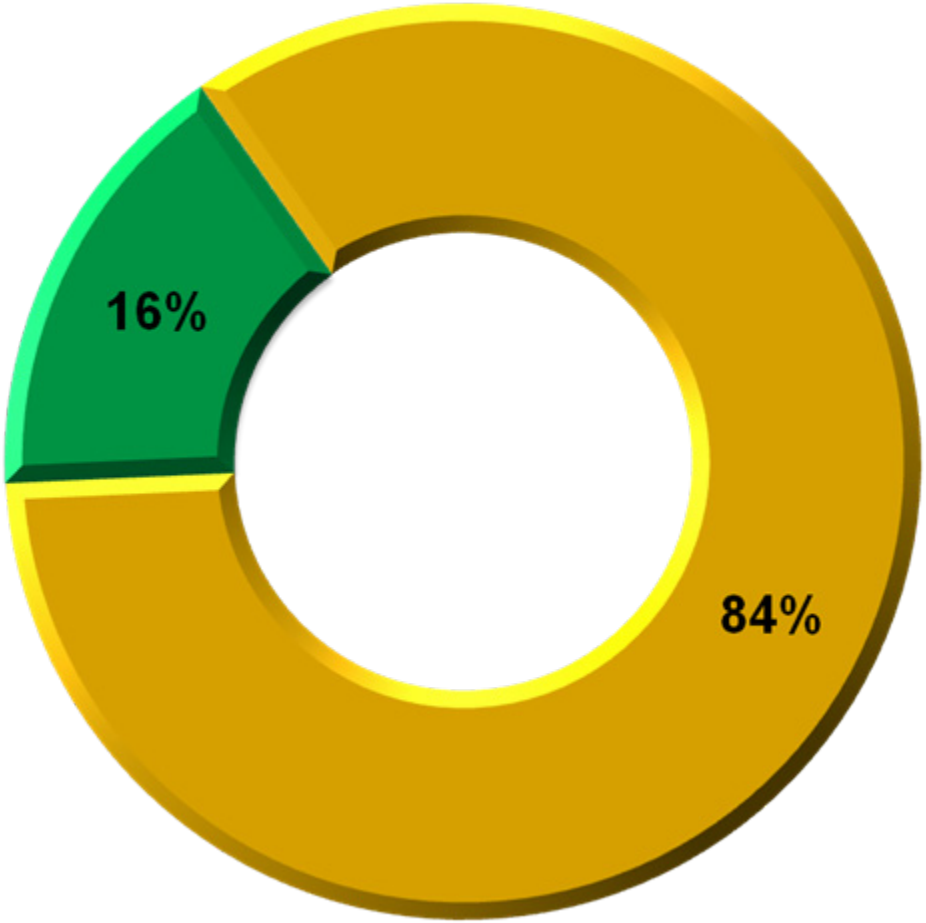
Незаконная деятельность в области защиты информации

УГОЛОВНЫЙ КОДЕКС РФ от 13 июня 1996 года N 63-ФЗ

Статья 137.
Нарушение неприкосновенности частной жизни

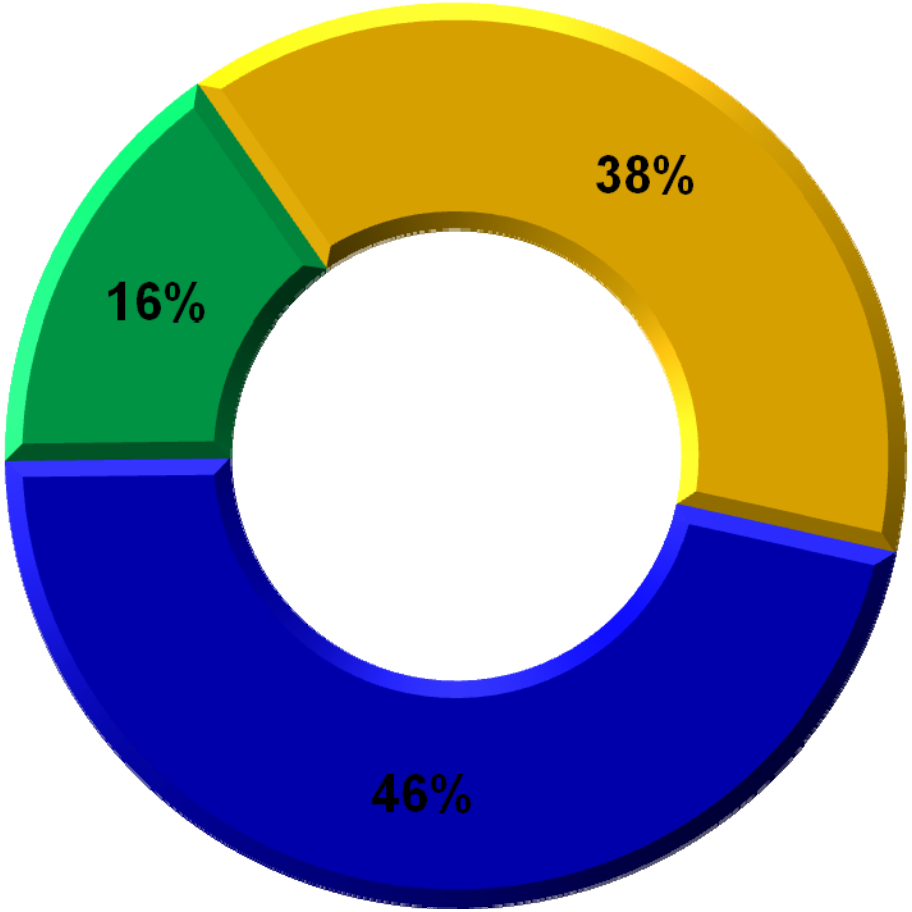
Статья 171.
Незаконное предпринимательство

Соотношение категорий информации подлежащих защите до выхода ФЗ №152



- Конфиденциальная информация
- Другая информация

Соотношение категорий информации подлежащих защите после выхода ФЗ №152



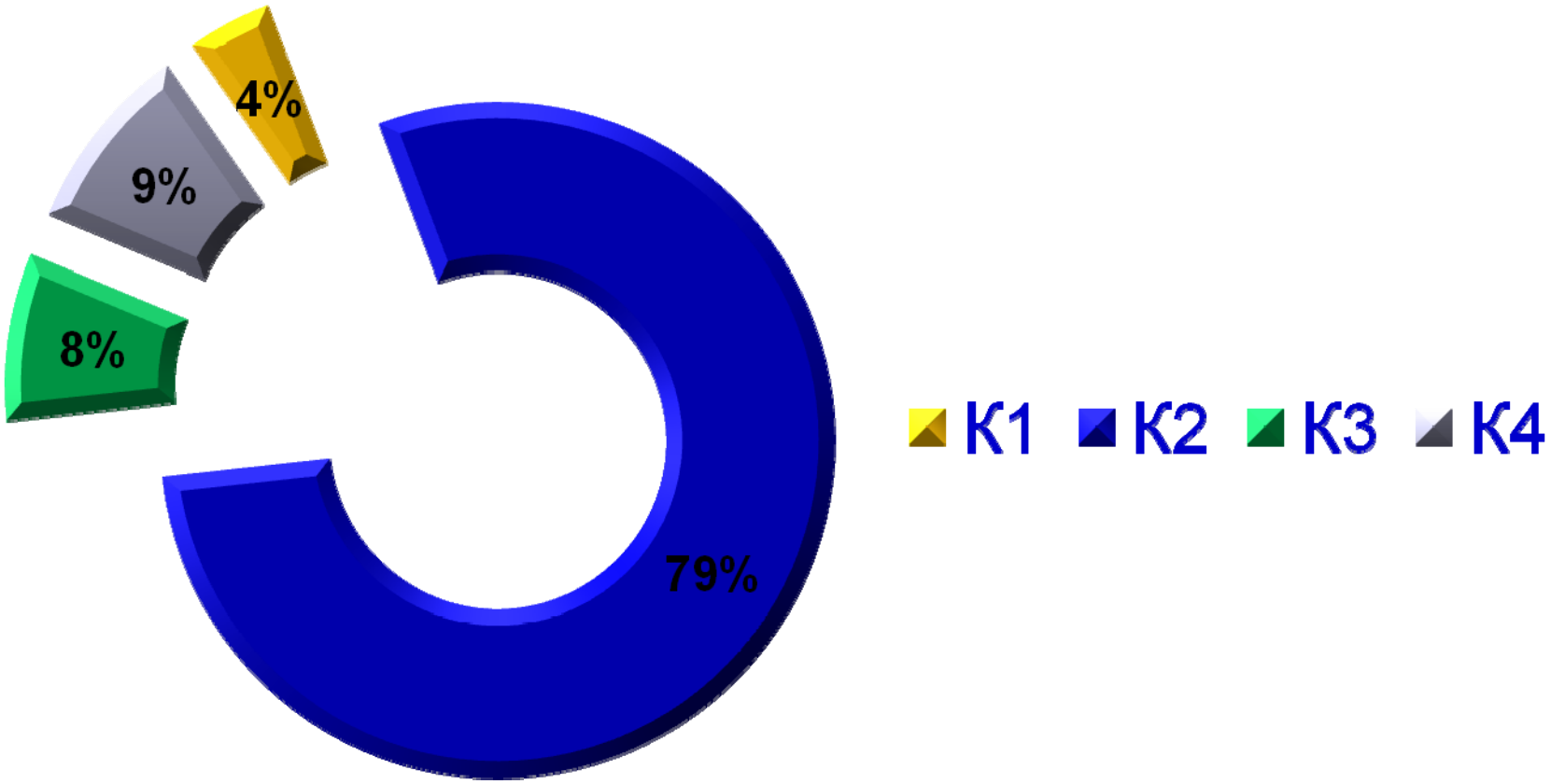
- Конфиденциальная информация
- Персональные данные
- Другая информация

Классификация ИСПДн

Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"

$X_{пд}$ \ $X_{нпд}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Соотношение классов ИСПДн

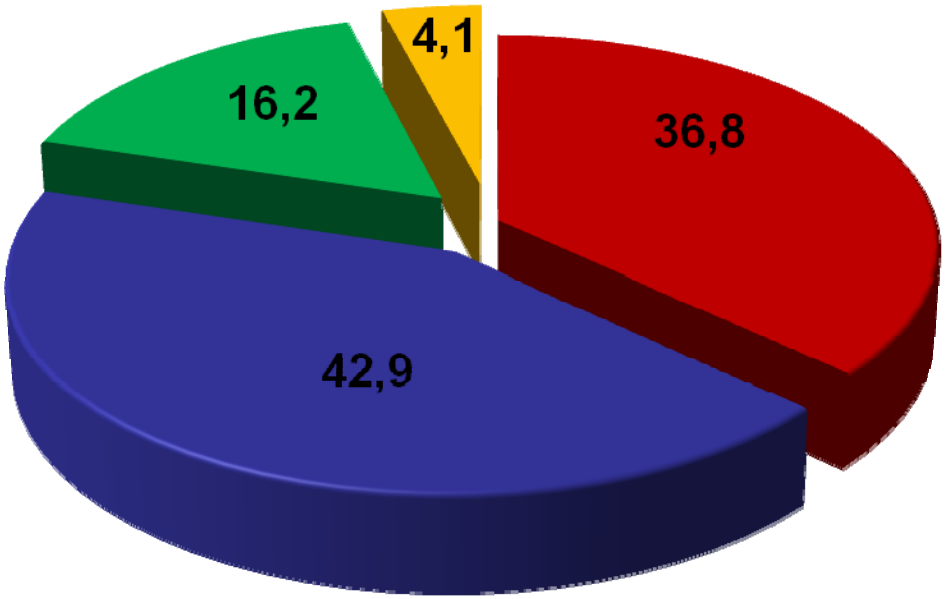


Заседание президиума Государственного совета Российской Федерации

17 июля 2008 года в Петрозаводске состоялось заседание президиума Государственного совета, на котором шла речь о реализации Стратегии развития информационного общества в Российской Федерации.

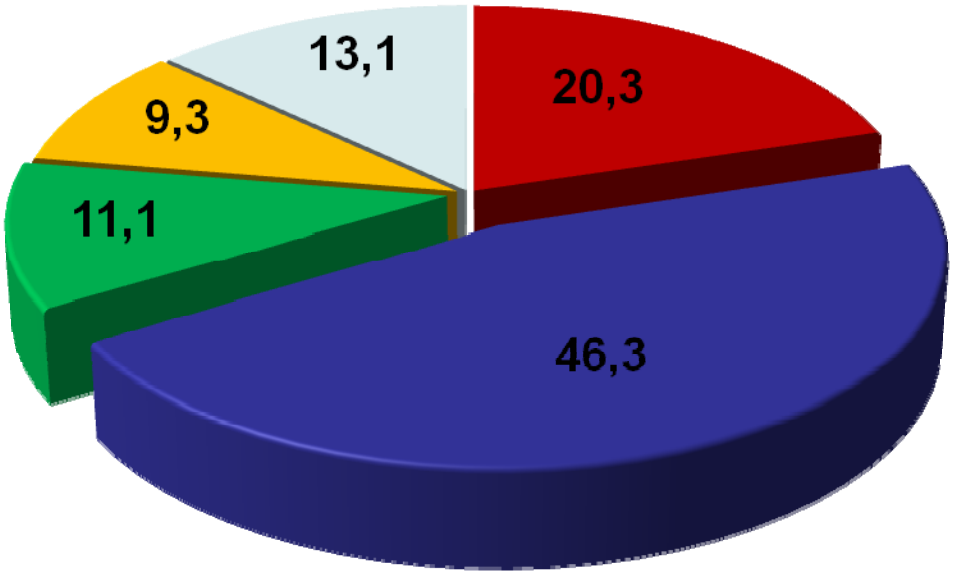
«… ещё одним вопросом в развитии информационных технологий остаётся безопасность. Всем пользователям мы должны обеспечивать и безопасный режим работы, и режим, который позволяет сохранять государственную тайну, коммерческую тайну и личную тайну.»

Осведомлённость специалистов о ФЗ №152



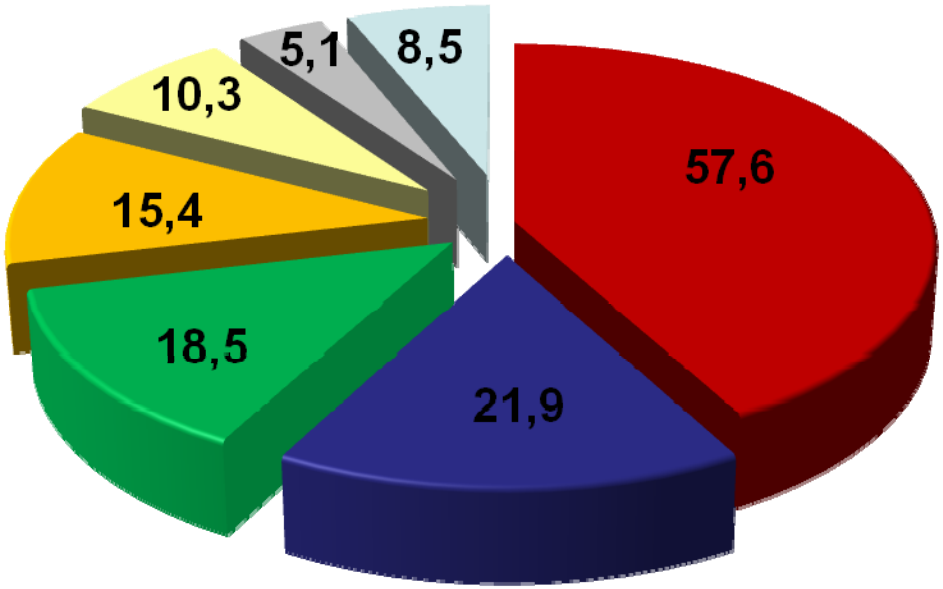
- Прекрасно осведомлён
- Знаком, но не вдавался в подробности
- Имею только общее представление
- Нет, не знаком

Соответствие требованиям ФЗ №152



- Все требования выполняются
- Требования выполняются частично
- Требования не выполняются
- Меры защиты ПД никак не связаны с ФЗ
- А что это за требования?

Кто имеет доступ к массивам ПДн



- Сотрудники службы безопасности и ИТ-службы
- Топ менеджеры или руководители ведущих подразделений
- Сотрудники аналитических служб
- Сотрудники других подразделений
- Сотрудники служб технической потдержки
- Только сотрудники службы безопасности
- Затрудняюсь ответить

«Разработка отечественного ПО обеспечит нашу информационную безопасность и будет способствовать существенной экономии средств»

ГК «Информзащита»

- Специализируется в области обеспечения информационной безопасности автоматизированных систем управления и более 10 лет является экспертом и одним из лидеров российского рынка ИБ.
- Разрабатывает программные и аппаратные комплексы для защиты конфиденциальной информации, персональных данных, государственной тайны. В феврале 2009 года производство выделено в отдельную компанию «Код безопасности»
- Компании группы и продукты собственного производства имеют необходимые лицензии и сертификаты:

- ✓ФСТЭК России
- ✓ФСБ России
- ✓Минобороны
- ✓СВР России

ГК «Информзащита»

Крупнейший российский специализированный холдинг ИБ, входящий в ТОП-100 крупнейших ИТ-компаний

- ✓ Средства защиты информации и бизнеса 2008 (за 2007) – 2 место
- ✓ Рейтинг C-News по безопасности 2007 - 2 место
- ✓Российские информационные и коммуникационные технологии, 2008 (РА ЭКСПЕРТ) – 36 место
- ✓CNews100: Крупнейшие ИТ-компании России 2007 (за 2007 год) – 52 место

Что мы защищаем?

Все элементы ИС, где обрабатывается, хранится или передается информация:

- ✓Автономные компьютеры
- ✓Рабочие станции и сервера ЛВС
- ✓Информация, передающуюся в ЛВС и по сетям общего пользования
- ✓Среды обработки данных (СУБД) и исполнения (виртуальные машины)

Какие средства защиты необходимо применять?

Защита ИСПДн в общем случае требует использования следующих сертифицированных защитных систем:

- ✓СЗИ от НСД
- ✓Межсетевые экраны
- ✓Антивирусные средства
- ✓Системы защиты от программно-математического воздействия
  - ✓ Обычно входят в состав антивирусных пакетов
- ✓Средства криптографической защиты
  - ✓ Применяется в случае защиты ИСПДн по требованиям ФСБ или когда в типовой системе разграничение доступа невозможно обеспечить средствами СЗИ от НСД

СЗИ от НСД

Средства защиты информации от несанкционированного доступа:

СЗИ Security Studio

- ✓ Агент конфиденциальности
- ✓ Агент контроля целостности

СЗИ Secret Net

Главное отличие – уровень целевой ИС

Требования	СЗИ Secret Net	СЗИ Security Studio	
		Агент конф-ти	Агент КЦ
АС	1Б	1Г	
ПД	**К1**	**К2**	**К3**

СЗИ Security Studio

СЗИ Security Studio - средство защиты информации от несанкционированного доступа, сочетающее в себе:

- ✓Полный набор необходимых механизмов защиты информации
- ✓Средства централизованного управления настройками защитных механизмов,
- ✓Средства оперативного реагирования на действия нарушителей
- ✓Возможность мониторинга безопасности защищаемой информационной системы в режиме реального времени.

Упрощает процесс аттестации автоматизированной системы организации до класса 1Г

Возможности СЗИ Security Studio

✓ Аутентификация:

- ✓ идентификация и аутентификация пользователей с использованием электронных идентификаторов;

✓ Управление доступом:

- ✓ управление доступом к конфиденциальной информации, основанное на неиерархических категориях конфиденциальности;
- ✓ контроль доступа субъектов к защищаемым информационным, программным и аппаратным ресурсам;

✓ Контроль целостности:

- ✓ контроль целостности данных и аппаратной конфигурации;

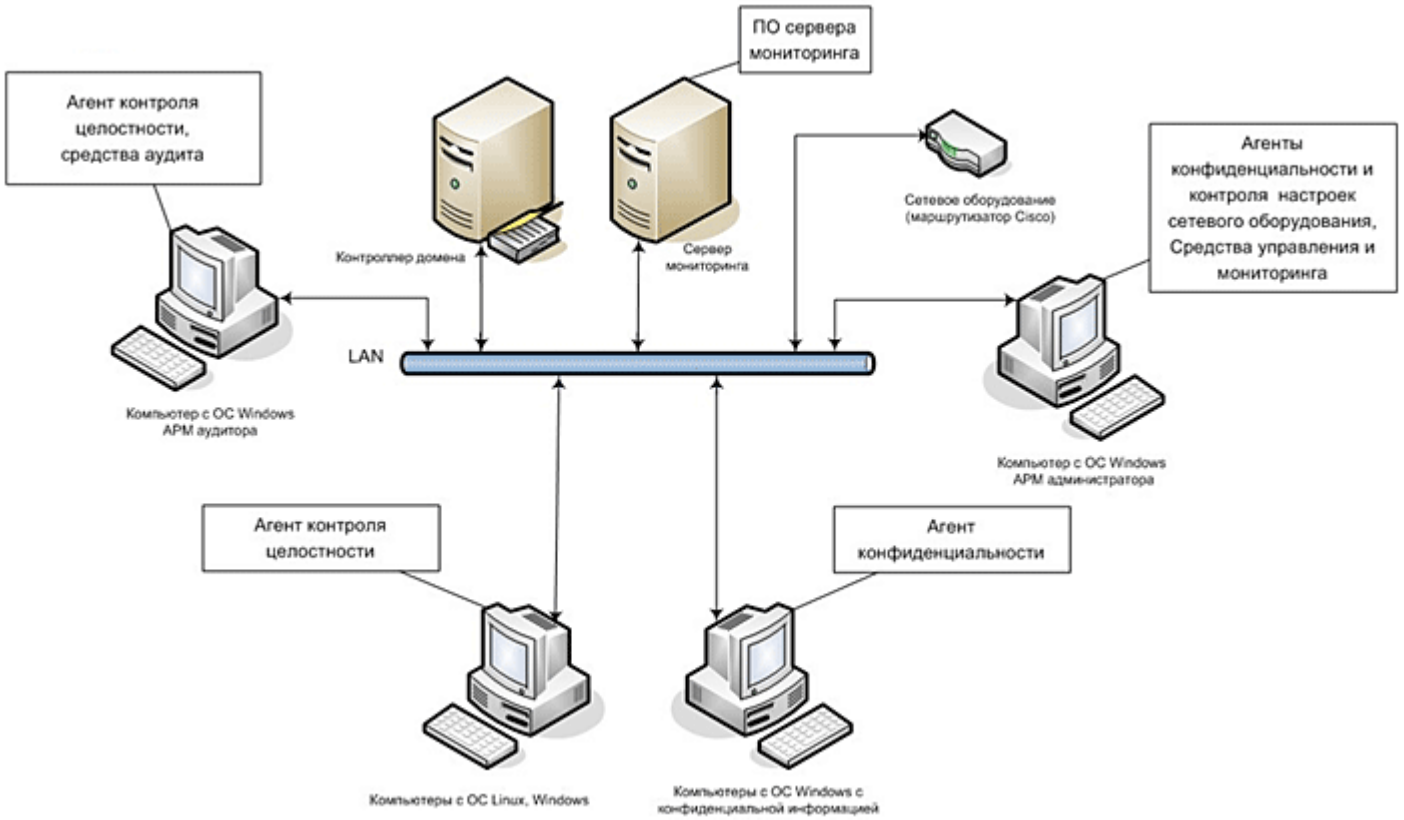
✓ Регистрация событий безопасности:

- ✓ регистрация и учет событий информационной безопасности;
- ✓ мониторинг состояния информационной системы;

✓ Другие возможности:

- ✓ аудит действий пользователей;
- ✓ временная блокировка работы компьютеров при наступлении события НСД;
- ✓ затирание остаточной информации.

СЗИ Security Studio



СЗИ Security Studio
Агент контроля целостности

Защита ИСПДн класса К3

СЗИ Security Studio Агент контроля целостности:

- ✓ Контроль целостности среды обработки данных:
  - ✓ контроль аппаратной конфигурации компьютеров
  - ✓ контроль настроек операционной системы, критичных приложений серверов и рабочих станций
- ✓ Аутентификация:
  - ✓ Идентификация и аутентификация пользователей, в том числе с использованием электронных идентификаторов eToken;
- ✓ Регистрация событий безопасности
  - ✓ Централизованный аудит и мониторинг событий безопасности

СЗИ Security Studio
Агент конфиденциальности

Защита ИСПДн класса К2

Добавляется требование по наличию дискреционного разграничения доступа (в том числе к устройствам).

СЗИ Security Studio Агент конфиденциальности:

✓Гибкое разграничение прав пользователей:
основанное на неиерархических метках конфиденциальности (до 50 меток);

✓Разграничение прав доступа пользователей к любому внутреннему и внешнему устройству:

- ✓ последовательные и параллельные порты,
- ✓ сменные, логические и оптические диски,
- ✓ USB–порты.

СЗИ Secret Net

СЗИ Secret Net – это система защиты конфиденциальной информации на серверах и рабочих станциях от несанкционированного доступа.

- ✓Организация разграничения доступа к конфиденциальной информации;
- ✓Контроль каналов распространения конфиденциальной информации;
- ✓Централизованное и оперативное управление информационной безопасностью.

Применяется для защиты гостайны и ИСПД до класса К1 включительно

СЗИ Secret Net

Защита ИСПДн класса К1

Для ИСПДн класса К1 СЗИ от НСД также должно реализовывать:

- ✓Мандатное управление доступом
- ✓Доверенную программную среду
- ✓Управление потоками конфиденциальной информации

СЗИ Secret Net закрывает все эти требования…

Возможности СЗИ Secret Net

- ✓ Разграничение доступа
  - ✓ Усиленная идентификация и аутентификация пользователей
  - ✓ Управление доступом пользователей к конфиденциальным данным
  - ✓ Разграничение доступа к устройствам
- ✓ Доверенная информационная среда
  - ✓ Защита от загрузки с внешних носителей
  - ✓ Замкнутая программная среда и контроль целостности
  - ✓ Функциональный самоконтроль подсистем
  - ✓ Контроль аппаратной конфигурации компьютера
- ✓ Защита информации в процессе хранения
  - ✓ Шифрование файлов
  - ✓ **Контроль печати конфиденциальной информации**
  - ✓ Гарантированное уничтожение данных
  - ✓ Регистрация событий
- ✓ Удобство управления и настроек
  - ✓ Централизованное управление и мониторинг
  - ✓ Импорт и экспорт параметров

СЗИ Secret Net

ПАК «Соболь»

СЗИ Secret Net требует использования платы аппаратной поддержки ПАК «Соболь» (программно-аппаратный комплекс, электронный замок), реализующей функции:

- ✓запрет загрузки компьютера с внешних носителей на аппаратном уровне;
- ✓контроль целостности ОС, прикладного программного обеспечения и файлов пользователя до загрузки ОС.

Необходимость использования ПАК «Соболь» обуславливается высокими требованиями к безопасности информационных систем, для которых предназначено СЗИ Secret Net.

ПАК «Соболь»

Обладает сертификатами ФСБ России и ФСТЭК России, которые обеспечивают возможность использования СЗИ ПАК «Соболь» для защиты информации, составляющей коммерческую или государственную тайну в автоматизированных системах с классом защищенности до 1Б включительно.

Готовятся к выходу

Средства защиты среды исполнения и обработки данных:

✓СЗИ Security Studio for DB

Средство защиты информации от несанкционированного доступа для информационных систем, использующих для хранения данных
СУБД MS SQL Server.

Предназначено для защиты коммерческой тайны и персональных данных в ИСПДн класса К3.

✓СЗИ Security Studio for Virtual Infrastructure

Средство защиты информации от несанкционированного доступа в виртуальных инфраструктурах на основе VMware VI3.5 / VI4.0.

Предназначено для защиты коммерческой тайны и персональных данных в ИСПДн классов К2 и К3.

АПКШ «Континент»

Аппаратно-программный комплекс «Континент»

Средство построения VPN-сетей + Межсетевой экран.

«Континент-mini»
для малых офисов

«Континент-1000»
высокопроизводительный

- Объединение локальных сетей предприятия в единую сеть через VPN;
- Подключение удаленных пользователей к VPN по защищенному каналу;
- Разграничение доступа между информационными подсистемами организации;
- Организация защищенного взаимодействия со сторонними организациями.

Получает сертификаты по требованиям ФСТЭК как МСЭ 3 класса.

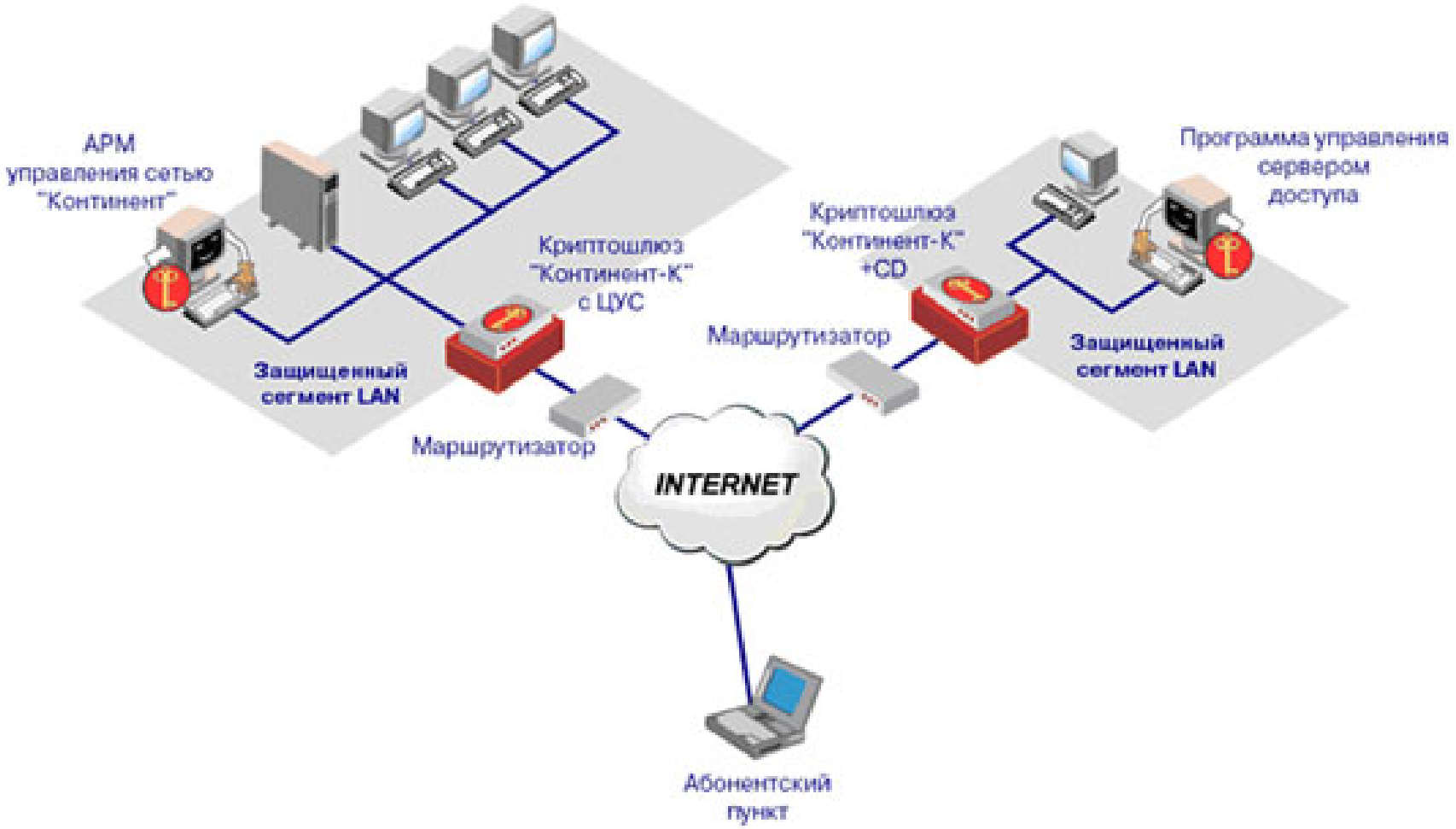
Может применяться, как сертифицированный МСЭ в ИСПДн до класса К1 включительно.

Средство защиты информации «Континент АП»

- ✓Программный продукт для организации VPN-доступа удаленных компьютеров к ресурсам локальной сети организации.
- ✓Объединяет средство построения VPN-сетей и Межсетевой экран
- ✓Функционирует в комплексе с АПКШ «Континент»

Сертифицирован ФСБ, как СКЗИ по КС1 и КС2.
Получает сертификат ФСТЭК, как МСЭ 3 класса.
Может применяться, как сертифицированное СКЗИ в ИСПДн до класса К1 включительно.

Межсетевые экраны



СКЗИ М-506А-XP

Программно-аппаратный комплекс, предназначенный для защиты информации в локальных вычислительных сетях

- **Защита информации от несанкционированного доступа**
  - ✓ (функции системы полностью аналогичны функциям СЗИ Secret Net);
- **Шифрование всего трафика ЛВС организации.**
  - ✓ Криптографическая защита данных, реализованная в соответствии с российским стандартом на криптографическую защиту информации ГОСТ 28147-89.

Обладает сертификатами ФСБ России, как СКЗИ, и может применяться для защиты информации, содержащей сведения, составляющие государственную тайну.
Может применяться, как сертифицированное СКЗИ в ИСПДн до класса К1 включительно.

СКЗИ М-506А-XP

Сводная таблица

Раздел требований		Продукт	К1	К2	К3
СЗИ от НСД	Защита среды исполнения	СЗИ **Secret Net**	●		
		СЗИ **Security Studio:** Агент конфиденциальности		●	
		СЗИ **Security Studio:** Агент контроля целостности			●
		СЗИ **Secret Net** for VMware Infrastructure	●		
		СЗИ **Security Studio** for VMware Infrastructure		●	●
	Защита среды обработки ПД	СЗИ **Secret Net** for DB	●		
		СЗИ **Security Studio** for DB: Агент конфиденциальности		●	
		СЗИ **Security Studio** for DB: Агент контроля целостности			●
	Аутентификация, КЦ, МДЗ	ПАК **«Соболь»**	●	●	
Межсетевое экранирование		АПКШ **«Континент» 3.5**	●	●	●
		СЗИ «**Континент АП**»	●	●	●
СКЗИ		СКЗИ **М-506А-XP**	●		

● - обязательные компоненты ● - возможные компоненты

Резюме

- ✓ СЗИ от НСД
  - СЗИ Secret Net
  - СЗИ Security Studio
    - ✓ Агент конфиденциальности
    - ✓ Агент контроля целостности
  - ПАК «Соболь»
  - СЗИ Security Studio for DB
  - СЗИ Security Studio for VI
- ✓ Межсетевые экраны
  - АПКШ «Континент»
  - СЗИ «Континент АП»
- ✓ СКЗИ
  - СКЗИ М-506А-XP

Все продукты сертифицированы ФСТЭК и/или ФСБ России

- В том числе по НДВ – это необходимо для использования СЗИ для защиты ПД
- В сертификатах явно прописана возможность использования в ИСПДн

Нам доверяют защиту своей информации

Центральный Банк
ГАС «Выборы»
Министерство финансов
Федеральное казначейство
ОАО «Вымпелком»
ОАО «Внешторгбанк»
Региональные управления Банка России и Сбербанка
Росэнергоатом
ГМК «Норильский никель»
и т.д.

Заказчики в регионе:

Национальный банк Удмуртии
СБ РФ в Удмуртии
Ижкомбанк
Ижевский государственный технический университет
И т.д.

ВОПРОСЫ?

Максим Илюхин

☎ (495) 980-2345
m.ilyukhin@infosec.ru