Информационная безопасность и защита информации в медицинском учреждении

Основные законы:

Об информации, информационных технологиях и о защите информации

Федеральный Закон № 149-ФЗ
от 27 июля 2006 года

О персональных данных

Федеральный Закон № 152-ФЗ
от 27 июля 2006 года

Об электронной подписи

Федеральный Закон № 63-ФЗ
от 6 апреля 2011 года

Информация – сведения (сообщения, данные)
независимо от формы их представления

Информационные технологии –
процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

Информационная система –
совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Информационно-телекоммуникационная сеть –
технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

«Об информации, информационных технологиях и о защите информации»
Федеральный Закон № 149-ФЗ от 27 июля 2006 года

Обладатель информации –
лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

Оператор информационной системы –
гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной

«Об информации, информационных технологиях и о защите информации»
Федеральный закон № 149-ФЗ от 27 июля 2006 года

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

«Об информации, информационных технологиях и о защите информации»
Федеральный Закон № 149-ФЗ от 27 июля 2006 года

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Об информации, информационных технологиях и о защите информации Федеральный Закон № 149-ФЗ от 27 июля 2006 года

Общедоступная информация

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

«Об информации, информационных технологиях и о защите информации»
Федеральный Закон № 149-ФЗ от 27 июля 2006 года

Общедоступная информация

Не может быть ограничен доступ к:

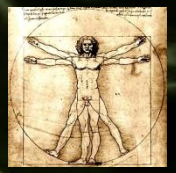
- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина;
- к информации о правовом положении, полномочиях и деятельности государственных органов, органов местного самоуправления и организаций; об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации о состоянии окружающей среды;
- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией.

«Об информации, информационных технологиях и о защите информации»
Федеральный Закон № 149-ФЗ от 27 июля 2006 года

Информация ограниченного доступа

Сведения, составляющие государственную тайну

Конфиденциальная информация

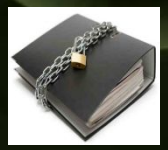


Персональные данные

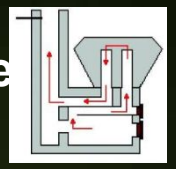
Сведения, связанные с профессиональной деятельностью

Сведения, составляющие коммерческую тайну

Тайна следствия



Служебная тайна



Сущность изобретения

Государственная тайна -

защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Закон РФ «О Государственной тайне»
N 5485-1 от 21 июля 1993 года

Конфиденциальная информация

- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (*персональные данные*)

- Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее)

- Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна)

Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» №188 от 6 марта 1997 г.

Конфиденциальная информация

- Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20.08.2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами РФ.

- Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).

- Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» №188 от 6 марта 1997 г.

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных

Федеральный Закон «О персональных данных» № 152-ФЗ от 27 июля 2006 года

Статья 6. Условия обработки персональных данных

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) осуществляется с согласия субъекта персональных данных

2) необходима для достижения целей, предусмотренных международным договором РФ или законом РФ

3) необходима для осуществления правосудия, исполнения судебного акта

4) необходима для предоставления государственной или муниципальной услуги в соответствии с 210-ФЗ от 27.07.2010 "Об организации предоставления государственных и муниципальных услуг", …для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) необходима для заключения (исполнения) договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных

Федеральный Закон «О персональных данных» № 152-ФЗ от 27 июля 2006 года

Статья 6. Условия обработки персональных данных

6) необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности…

9) осуществляется в статистических или иных исследовательских целях… при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Федеральный Закон «О персональных данных» № 152-ФЗ от 27 июля 2006 года

Статья 13. Соблюдение врачебной тайны

1. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

2. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных частями 3 и 4 настоящей статьи.

3. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

Федеральный Закон «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ от 21 ноября 2011 г

Статья 13. Соблюдение врачебной тайны

4. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю если медицинское вмешательство необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют законные представители

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия…

4) в случае оказания медицинской помощи несовершеннолетнему при оказании ему наркологической помощи или при медицинском освидетельствовании в целях установления состояния наркотического либо иного токсического опьянения, а также несовершеннолетнему, не достигшему 15 (16) лет;

5) в целях информирования органов внутренних дел о поступлении пациента при наличии подозрений о противоправных действиях

Федеральный Закон «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ от 21 ноября 2011 г

Статья 13. Соблюдение врачебной тайны

4. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом.

Федеральный Закон «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ от 21 ноября 2011 г

Статья 13. Соблюдение врачебной тайны

4. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом.

Федеральный Закон «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ от 21 ноября 2011 г

Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью.

Федеральный Закон «О персональных данных»
№ 152-ФЗ от 27 июля 2006 года

Согласие в письменной форме должно включать в себя, в частности:

1) ФИО, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) ФИО, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или ФИО и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или ФИО и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

Федеральный Закон «О персональных данных»
№ 152-ФЗ от 27 июля 2006 года

В _____
(наименование органа исполнительной власти
_____
субъекта Российской Федерации
_____
в сфере здравоохранения)
_____

ЗАЯВЛЕНИЕ
о согласии на обработку персональных данных

Я, _____,
(фамилия, имя, отчество (при наличии))
даю согласие _____
(наименование органа исполнительной власти субъекта Российской Федерации в сфере здравоохранения)
на обработку и использование данных, содержащихся в настоящем заявлении, с целью организации оказания высокотехнологичной медицинской помощи.

1. Дата рождения _____
(число, месяц, год)

2. Пол _____
(женский, мужской – указать нужное)

3. Документ, удостоверяющий личность _____
(наименование, номер и серия,
_____
кем и когда выдан)

4. Адрес по месту жительства _____
(почтовый адрес по месту жительства)
_____

5. Адрес фактического проживания _____
(почтовый адрес фактического проживания, контактный телефон)
_____

6. Серия, № полиса обязательного медицинского страхования (при наличии), наименование страховой медицинской организации, осуществляющей деятельность в сфере обязательного медицинского страхования _____

7. Страховой номер индивидуального лицевого счета (СНИЛС) (при наличии)
_____

8. Сведения о законном представителе
_____
(фамилия, имя, отчество)
_____
(почтовый адрес места жительства, фактического проживания, телефон)

9. Дата рождения законного представителя _____
(число, месяц, год)

10. Документ, удостоверяющий личность законного представителя
_____
(наименование, номер и серия, кем и когда выдан)
_____

11. Документ, подтверждающий полномочия законного представителя _____
_____
(наименование, номер и серия, кем и когда выдан)

Примечание. Пункты с 8 по 11 настоящего заявления заполняются в том случае, если заявление заполняет законный представитель гражданина Российской Федерации.

На передачу лично мне сведений о дате госпитализации и иных данных по телефонам, указанным в настоящем заявлении, согласен (согласна).
(нужное подчеркнуть)
Данные, указанные в заявлении, соответствуют представленным документам.

Заявление и документы гражданина (гражданки) _____
зарегистрированы _____
(№ Талона на оказание ВМП)

Принял

_____ _____ _____
(Ф.И.О. специалиста) (дата приема заявления) (подпись специалиста)

(линия отреза)

Расписка-уведомление

Заявление и документы гражданина (гражданки) _____
_____
(№ Талона на оказание ВМП)
Принял

_____ _____ _____
(Ф.И.О. специалиста) (дата приема заявления) (подпись специалиста)

Приложение № 9 к приказу Министерства здравоохранения и социального развития Российской Федерации № 212н от 11 марта 2012 г.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
   1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
   2) соблюдение конфиденциальности информации ограниченного доступа;
   3) реализацию права на доступ к информации.
2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации...
3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

.

«Об информации, информационных технологиях и о защите информации»
Федеральный Закон № 149-ФЗ от 27 июля 2006 года

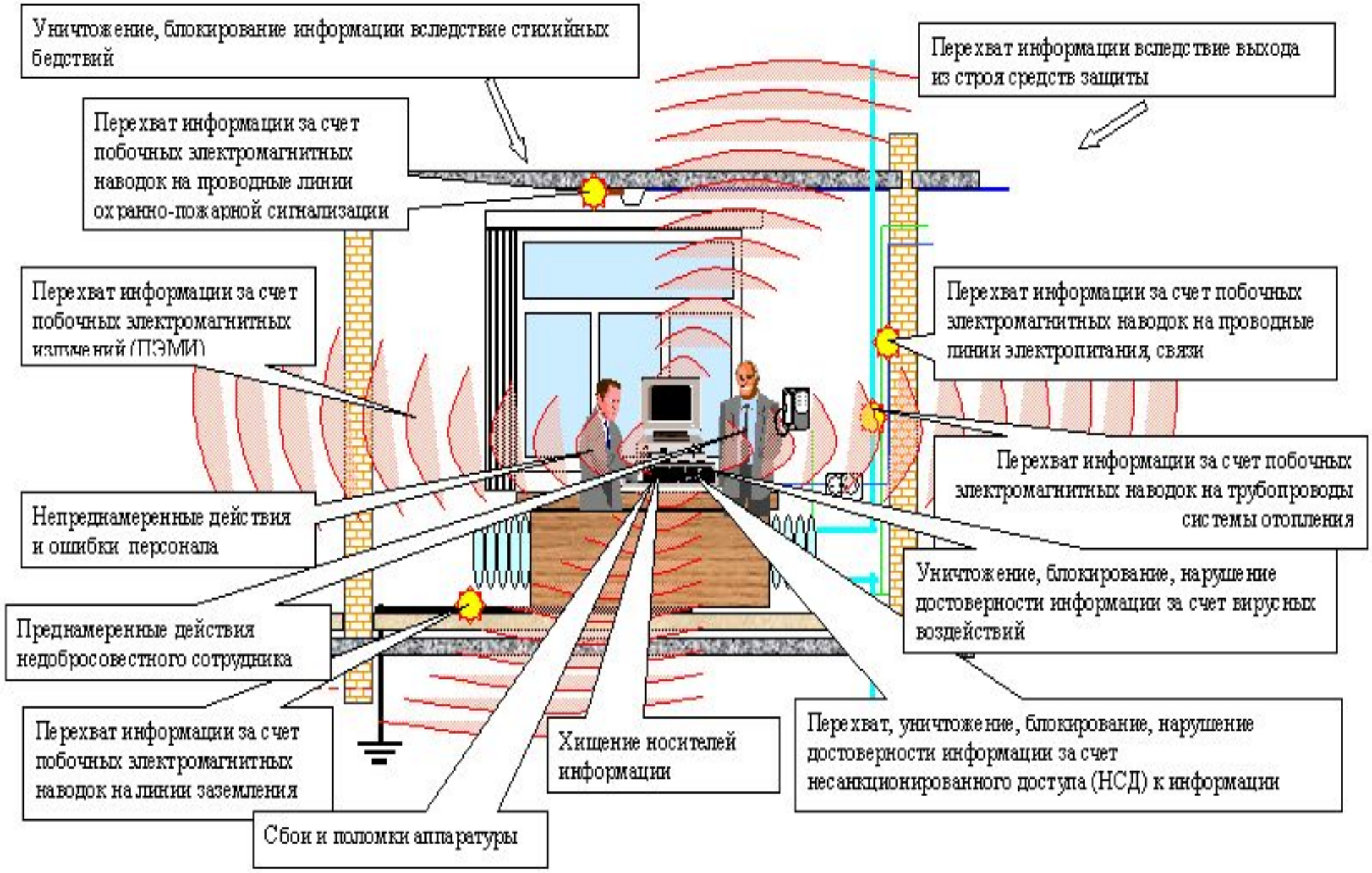
Статья 16. Защита информации

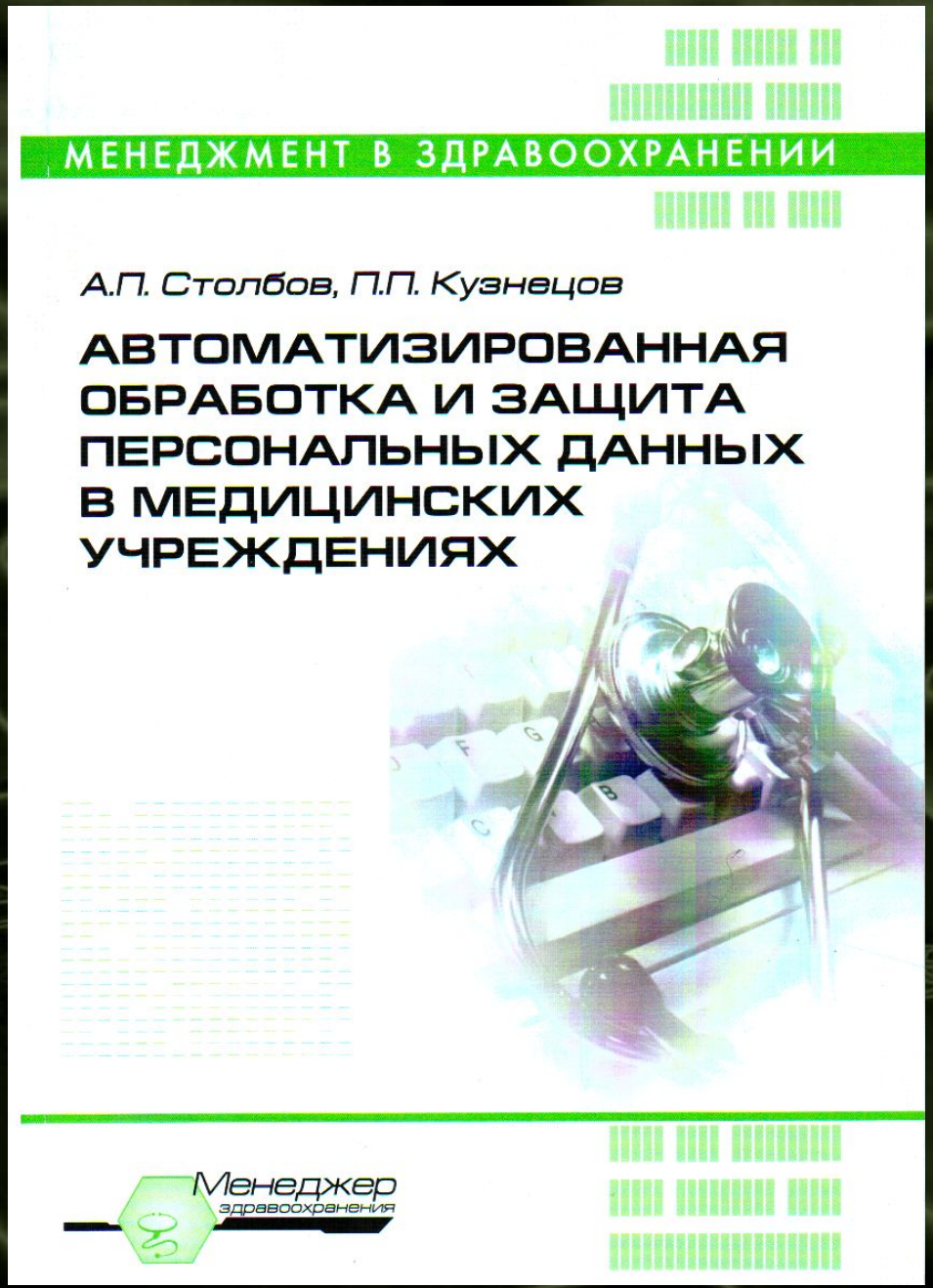
4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2) своевременное обнаружение фактов несанкционированного доступа к информации;
3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) контроль за обеспечением уровня защищенности информации.

«Об информации, информационных технологиях и о защите информации»
Федеральный Закон № 149-ФЗ от 27 июля 2006 года

Технические каналы утечки и воздействия на информацию при обработке ее техническими средствами





Андрей Павлович Столбов
доктор технических наук,
профессор,
заместитель директора
МИАЦ РАМН.

Пётр Павлович Кузнецов
доктор медицинских наук,
профессор,
директор МИАЦ РАМН.

Министерство здравоохранения и социального развития Российской Федерации

СОГЛАСОВАНО

Начальник 2 управления ФСТЭК России

_____ А.В. Куц

«12» декабря 2009 г.

УТВЕРЖДАЮ

Директор Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации

_____ О.В. Симаков

«23» декабря 2009 г.

Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

Москва 2009

Модель угроз
типовой медицинской информационной системы (МИС)
типового лечебно профилактического учреждения
(ЛПУ)

Министерство здравоохранения и социального развития Российской Федерации

СОГЛАСОВАНО

Начальник 2 управления ФСТЭК России

_____ А.В. Куц

«12» декабря 2009 г.

УТВЕРЖДАЮ

Директор Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации

_____ О.В. Симаков

«23» декабря 2009 г.

Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости

Москва 2009

Актуальные угрозы безопасности ПДн

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

«Требования к защите персональных данных при их обработке в информационных системах персональных данных».
Утверждены постановлением Правительства РФ от 1 ноября 2012 г. № 1119

Виды угроз 3-го типа

A – обусловленные случайными человеческими действиями – ошибки пользователей, неисправности в системе вентиляции, электро- и водоснабжения, недостаточная численность персонала, и пр.

E – обусловленные естественными (природными) причинами – ураган, землетрясение, молния, и пр.

D – обусловленные преднамеренными действиями – кража, несанкционированный доступ, намеренное повреждение, перехват информации, анализ трафика, несанкционированное использование ПО, и пр.

ГОСТ Р ИСО/МЭК ТО 13335-3—2007
«Информационная технология. Методы и средства обеспечения безопасности»

Информационная безопасность должна обеспечивать *сохранность* информации и предотвращать:

- утрату,
- блокирование,
- искажение,
- подделку,
- несанкционированный доступ (не связанный с выполнением функциональных обязанностей и не оформленный документально);
- хищение (несанкционированное копирование) информации.

Что и где «протекает» ?

В Японии украдены персональные данные более 10 млн человек. Токийская полиция арестовала пять человек по подозрению в создании и распространении бесплатных приложений для смартфонов, через которые злоумышленники получили доступ к персональным данным более 10 миллионов человек.

Программы были доступны для скачивания в виде популярных игр-приложений для телефонов, использующих операционную систему Android. Они были созданы таким образом, что после установки программа передает все данные из адресной книги пользователя на сервер.

Согласно материалам следствия, с февраля 2012 года злоумышленники разместили в интернете около 50 подобных приложений.

Что и где «протекает» ?

Бывший майор полиции Владислав Смирнов, работавший в информационном центре МВД, пойдет под суд за вмешательство в частную жизнь и разглашение персональных данных граждан. Дело в отношении Владислава Смирнова возбудили в июне 2012 г. на основании оперативных материалов УФСБ по Новосибирской области.

Майор МВД предоставлял новосибирским детективным агентствам информацию об интересующих их предпринимателях. Агентства в свою очередь передавали информацию заказчикам - коммерческим предприятиям, проверявшим деятельность деловых партнеров. Согласно материалам дела, полицейский передал частным детективам данные более чем о пятидесяти предпринимателях.

Что и где «протекает» ?

Facebook начал расследование, каким образом болгарский блоггер и борец за права интернет-пользователей Богомил Шопов купил персональные данные 1,1 млн пользователей Facebook, включая имена пользователей, ID их страниц в соцсети и их личные адреса электронной почты, сообщает американский Forbes.

По словам болгарского блоггера, он проверил данные из нескольких аккаунтов и адресов электронной почты – они оказались реально действующими, причем купленные им e-mail не отображались на страницах пользователей соцсети в публичном доступе. Он также сообщил, что эти данные он купил на сайте компании Gigbucks всего за $5.

Виды нарушителей

Внешние

- Разведывательные службы государств;
- Криминальные структуры;
- Конкуренты (конкурирующие организации);
- Недобросовестные партнеры;
- Внешние субъекты (физические лица).

Внутренние

- Зарегистрированные пользователи;
- Лица, имеющие санкционированный доступ к ИС, но не имеющие доступа к информации (системные администраторы);
- Программисты-разработчики (поставщики) ПО и лица, обеспечивающие его сопровождение ;
- Лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИС.

2 важнейших принципа обеспечения информационной безопасности:

1. Принцип враждебности окружения
2. «Запрещено все, что не разрешено»

Как будем защищать ?

Фундаментальная проблема

Защищенность

Удобство

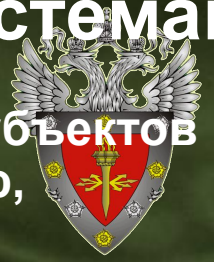
Дешевизна

Защищенная система отличается от всех прочих в первую очередь тем, что рассматривает проблему обеспечения безопасности информационных систем как лежащую на стыке двух направлений: общей безопасности и автоматизации обработки информации.

- Въезд на территорию
- Вход в здание
- Внутренняя система разграничения доступа и слежения

- Вход в компьютер и в ЛВС
- Вход в информационную систему
- Система разграничения доступа и слежения

Общие требования к информационным системам



1. Идентификация, проверка подлинности и контроль доступа субъектов (пользователей) в систему по идентификатору (коду) и паролю, длиной не менее шести буквенно-цифровых символов.
2. Регистрация и учет входа (выхода) субъектов доступа в (из) системы (узел сети), включающая: дату и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.
3. Физическая охрана средств вычислительной техники и носителей информации, предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС.
4. Учет носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку компьютера).
5. Обеспечение целостности программных средств и обрабатываемой информации.
6. Периодическое тестирование средств защиты информации от несанкционированного доступа.
7. Наличие средств восстановления средств защиты информации от несанкционированного доступа.

Идентификация (лат. *Identifico* — отождествлять) в компьютерной безопасности — процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом.

Аутентификация (англ. *Authentication*) или подтверждение подлинности — процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации.

Авторизация (англ. *Authorization*) — процесс, а также результат процесса проверки (через идентификацию или аутентификацию) некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом.

Парольная защита

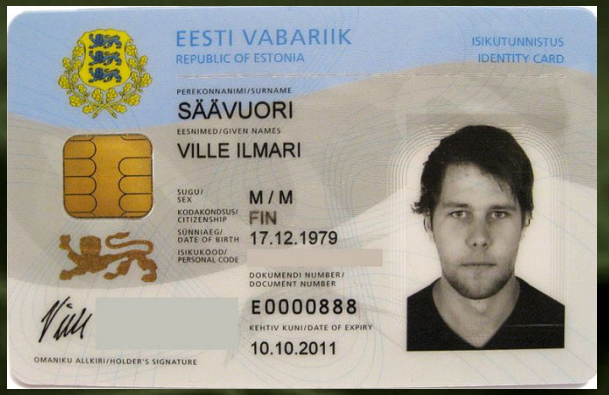
- Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после его идентификации и аутентификации по псевдониму (логину) и паролю.
- В качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность её угадывания.
- Пароль должен легко запоминаться.
- Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем

Парольная защита

- Выдачу пользователем паролей должен производить администратор информационной системы, который ведет "Журнал смены личных паролей".
- Внеплановая смена (удаление) личного пароля любого пользователя автоматизированной системы должна производиться в случае прекращения его полномочий (увольнение, либо переход на другую работу) немедленно после окончания последнего сеанса работы данного пользователя системы.
- Внеплановая полная смена всех паролей должна производится в случае прекращения полномочий администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.
- Для организации своевременной и эффективной парольной защиты необходимо внесение записи – отметки о блокировании (удалении) пароля в обходной лист увольняемого сотрудника.

Двухфакторная защита

Смарт-карты врача и пациента, используемые в системе здравоохранения Германии



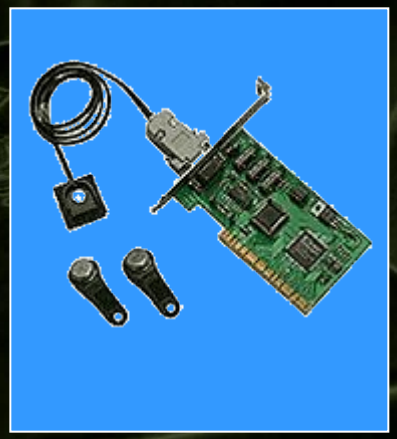
Идентификационная смарт-карта гражданина Эстонии

Социальная карта жителя Красноярского края

Контактный считыватель смарт-карт, подключаемые через порт USB

Двухфакторная защита

iButton —
семейство микроэлектронных устройств
фирмы Dallas Semiconductor (USA)



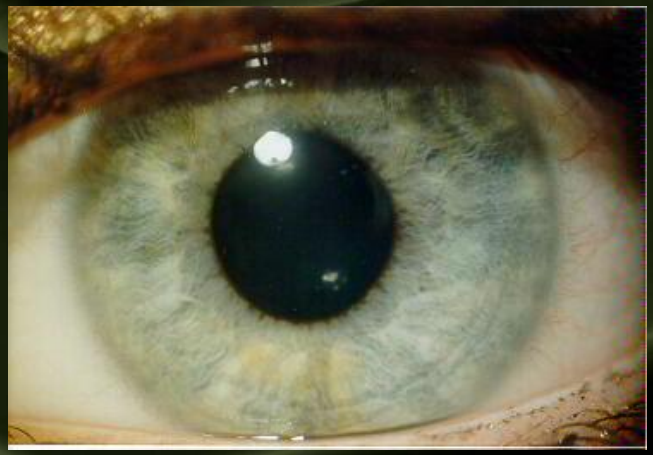
Программно – аппаратные
средства защиты информации,
сертифицированные Гостехкомиссией России
(«Аккорд - АМДЗ», «Криптон - замок/PCI»,
электронные замки «Соболь»).

Биометрическая аутентификация личности

Отпечатки пальцев

Биометрическая аутентификация личности

Аутентификации личности с помощью биометрического считывателя HandKey



Сканирование радужной оболочки или глазного дна

Биометрическая аутентификация личности

Оценка индивидуальных черт лица

Права доступа к информации —

совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и её носителям, установленных правовыми документами или собственником, владельцем информации.
Права доступа определяют набор действий (чтение, запись, выполнение), разрешённых для выполнения субъектам (пользователям системы) над объектами данных.
Система разграничения доступа (СРД) субъектов к объектам рассматривается в качестве главного средства защиты от НСД к информации по РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

VPN (_Virtual Private Networks_, виртуальная частная сеть) - технология безопасной передачи данных по каналам Интернет

Защищенные каналы – шифруется весь передаваемый и расшифровывает весь принимаемый трафик.

Частные каналы – трафик шифруется так же, как и для защищенного канала, но соединение требует аутентификации отправителя.

Промежуточные каналы – используются для промежуточной передачи зашифрованного трафика между двумя VPN.

Права доступа могут быть:

-персональными, то есть предоставленными сотруднику лично;

-должностными, то есть предоставленными сотруднику в соответствии с занимаемой им должностью (лечащий врач, зав. отделением, нач.мед. и др.);

-ситуационными (ролевыми), то есть отвечающими той ситуации (роли), в которой сотрудник исполняет свои обязанности (например, дежурный врач на время дежурства должен иметь больше прав, чем врач отделения; врач-консультант только при проведении консультации или врач-лаборант при выполнении исследования может получать полный доступ ко всем ЭПМЗ пациента);

- административными, то есть расширенными правами доступа, предоставленными специальному персоналу, осуществляющему администрирование медицинских архивов и ЭПМЗ, обеспечивающему безопасность и разрешение нештатных ситуаций.

Необходимость криптографической защиты конфиденциальной информации
(как подлежащей обязательной защите, так и не подлежащей обязательной защите) при ее обработке, хранении и передаче по каналам связи в случае отсутствия обмена конфиденциальной информацией с государственными органами, государственными организациями или другими организациями, выполняющими государственные оборонные заказы, и выбор типа СКЗИ определяются ее пользователем (в случае, если собственником информационных ресурсов или уполномоченным им лицом предварительно не определена необходимость криптографической защиты конфиденциальной информации и не выбран требуемый тип СКЗИ).

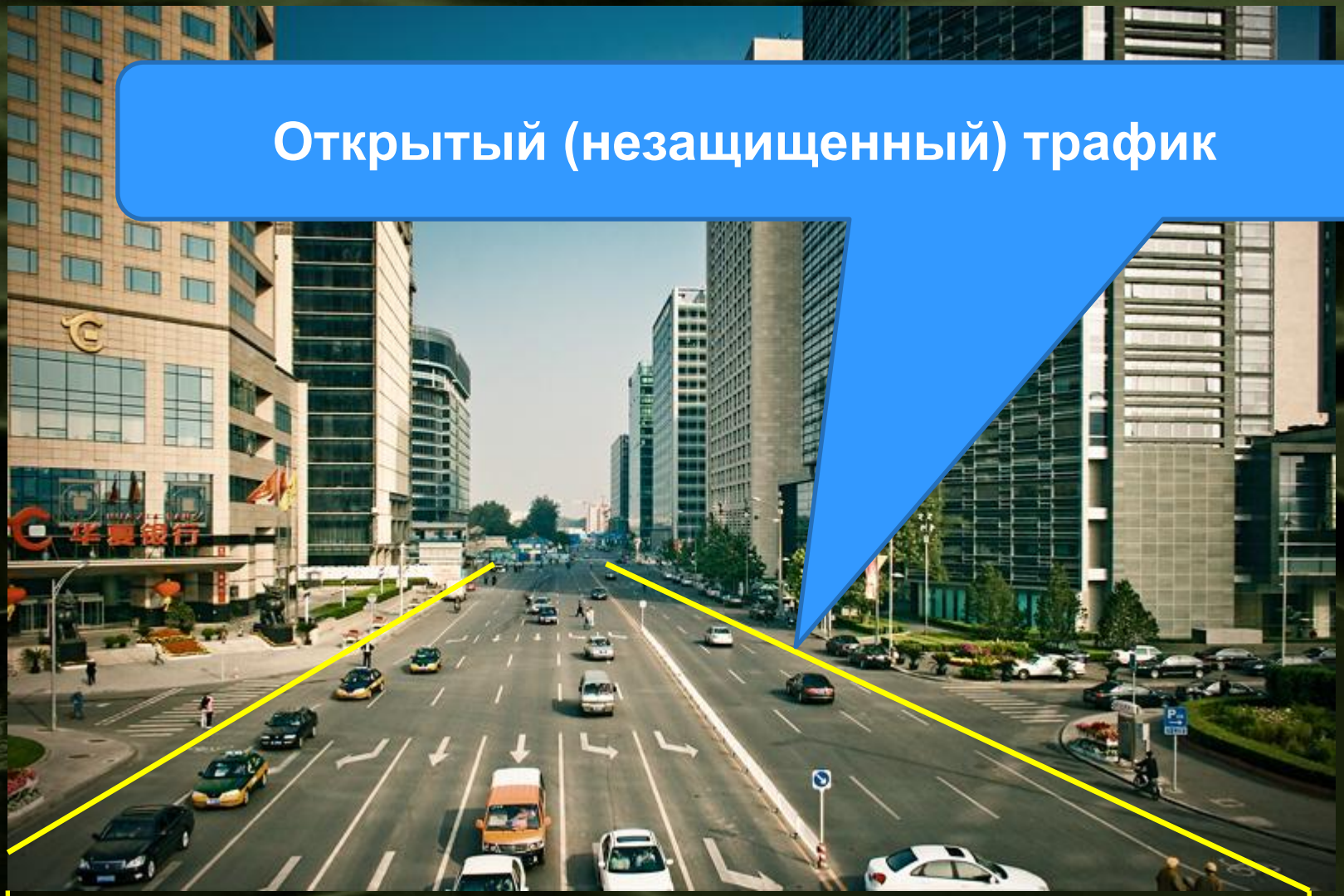
Положение «ПКЗ-99»
Утверждено Приказом ФАПСИ при Президенте РФ от 23.09.1999 № 158

Технологии безопасной передачи данных

VPN **(*Virtual Private Networks*, виртуальная частная сеть) – создание нескольких соединений (логической сети) поверх другой сети (Интернет)**

Технологии безопасной передачи данных

Технологии безопасной передачи данных



Технологии безопасной передачи данных

Технологии безопасной передачи данных

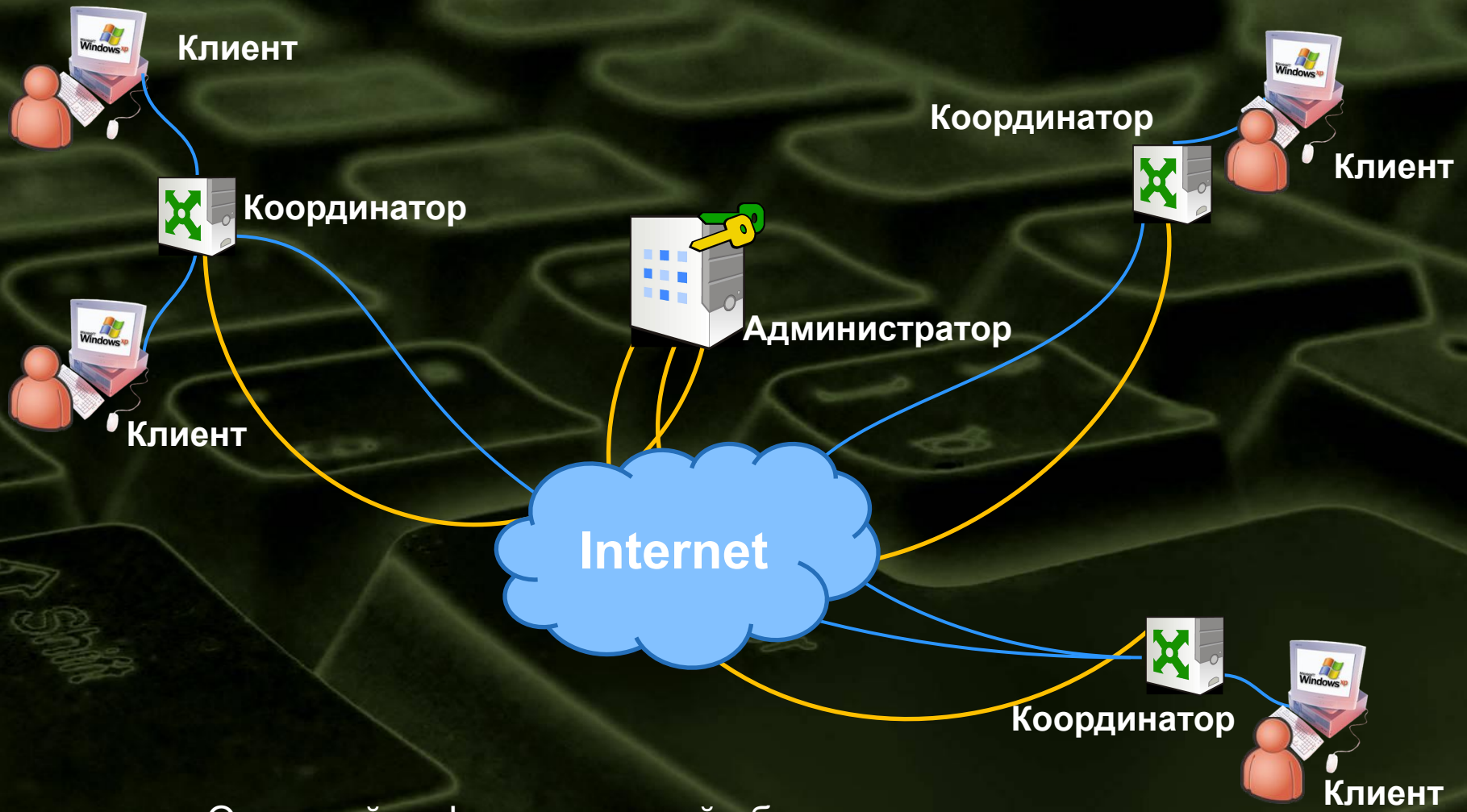
ViPNet состоит из 3-х основных программных модулей:

ViPNet Клиент – устанавливается на компьютер каждого пользователя, обеспечивает защищенное соединение с другими пользователями и защиту самого компьютера от сетевых атак

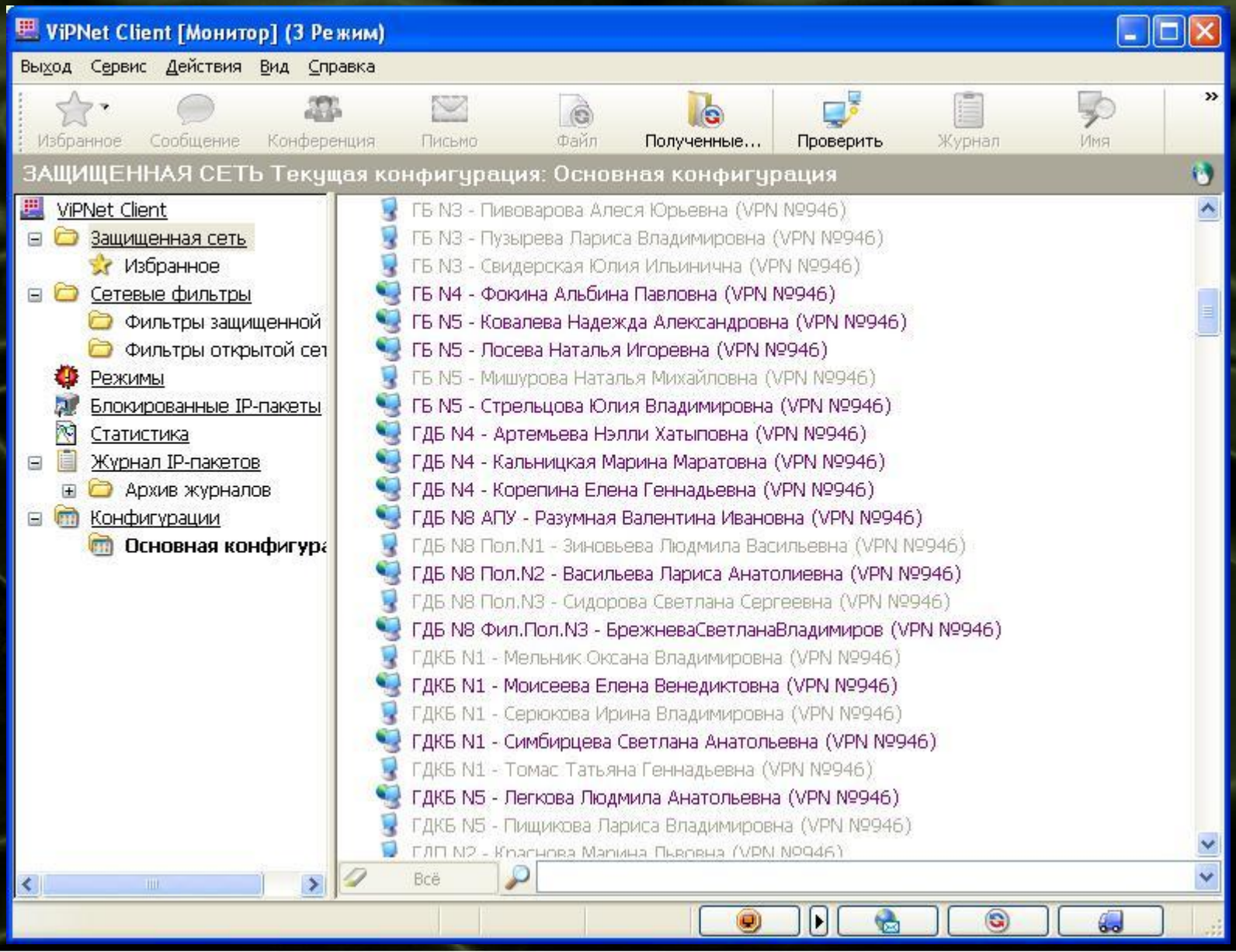
ViPNet Координатор – VPN-сервер с интегрированным межсетевым экраном, защищенным почтовым сервером и туннельным сервером для защищенных соединений.

ViPNet Администратор – центр управления сетью с функциями Удостоверяющего Центра

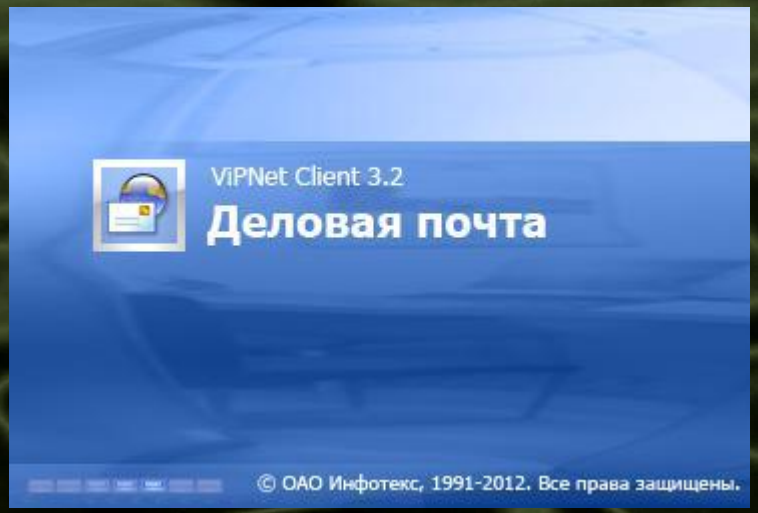
Схема сети ViPNet



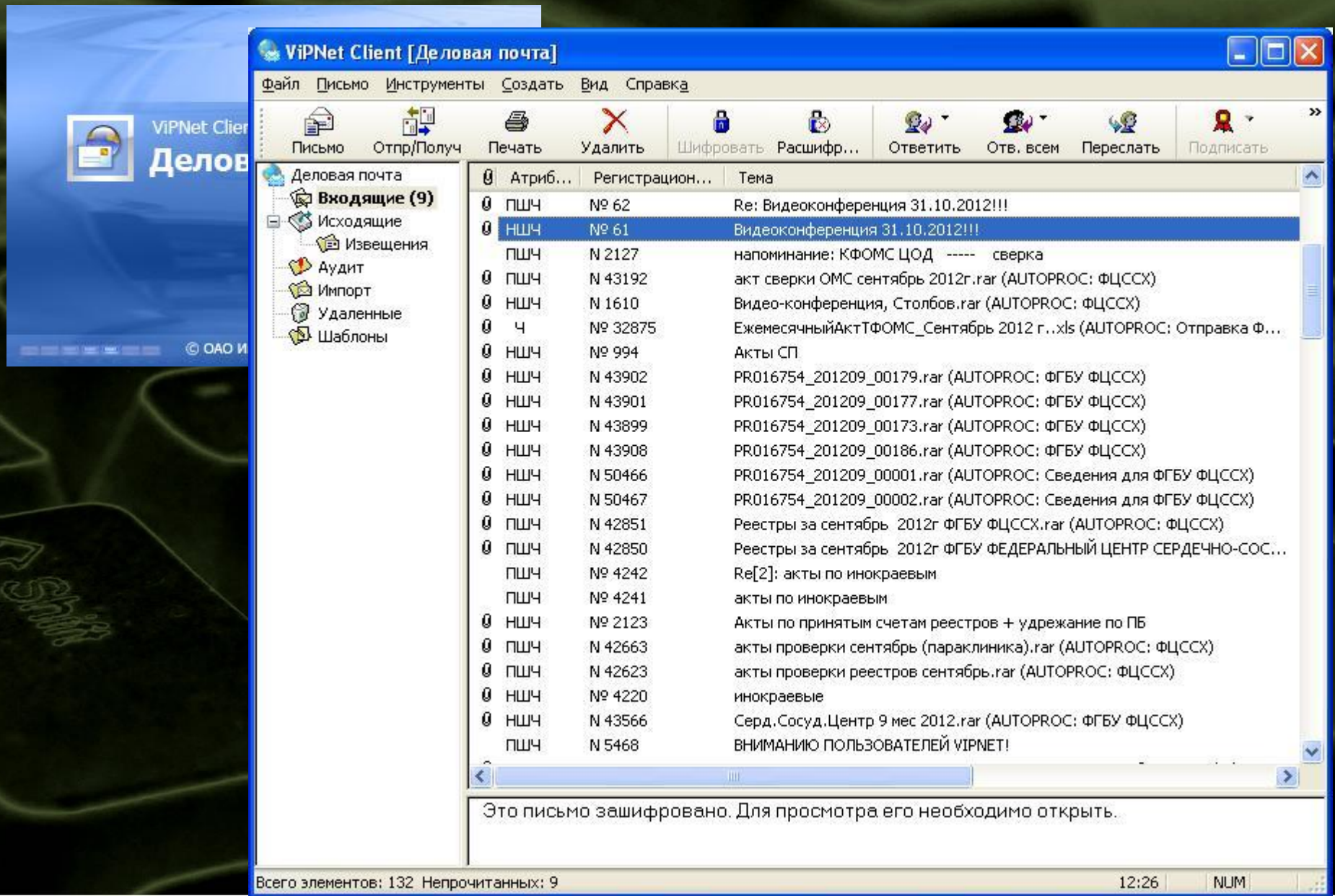
ViPNet-клиент: монитор сети



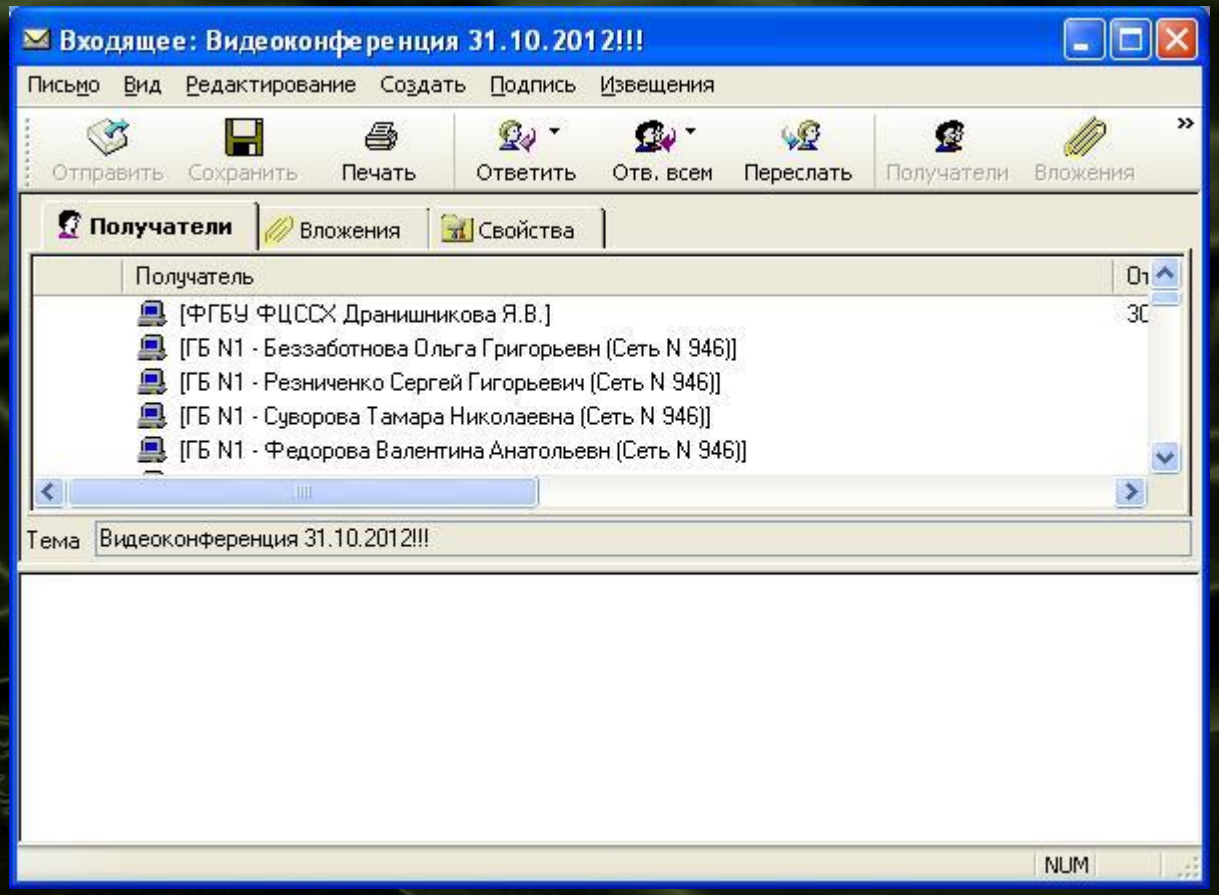
ViPNet-клиент: деловая почта



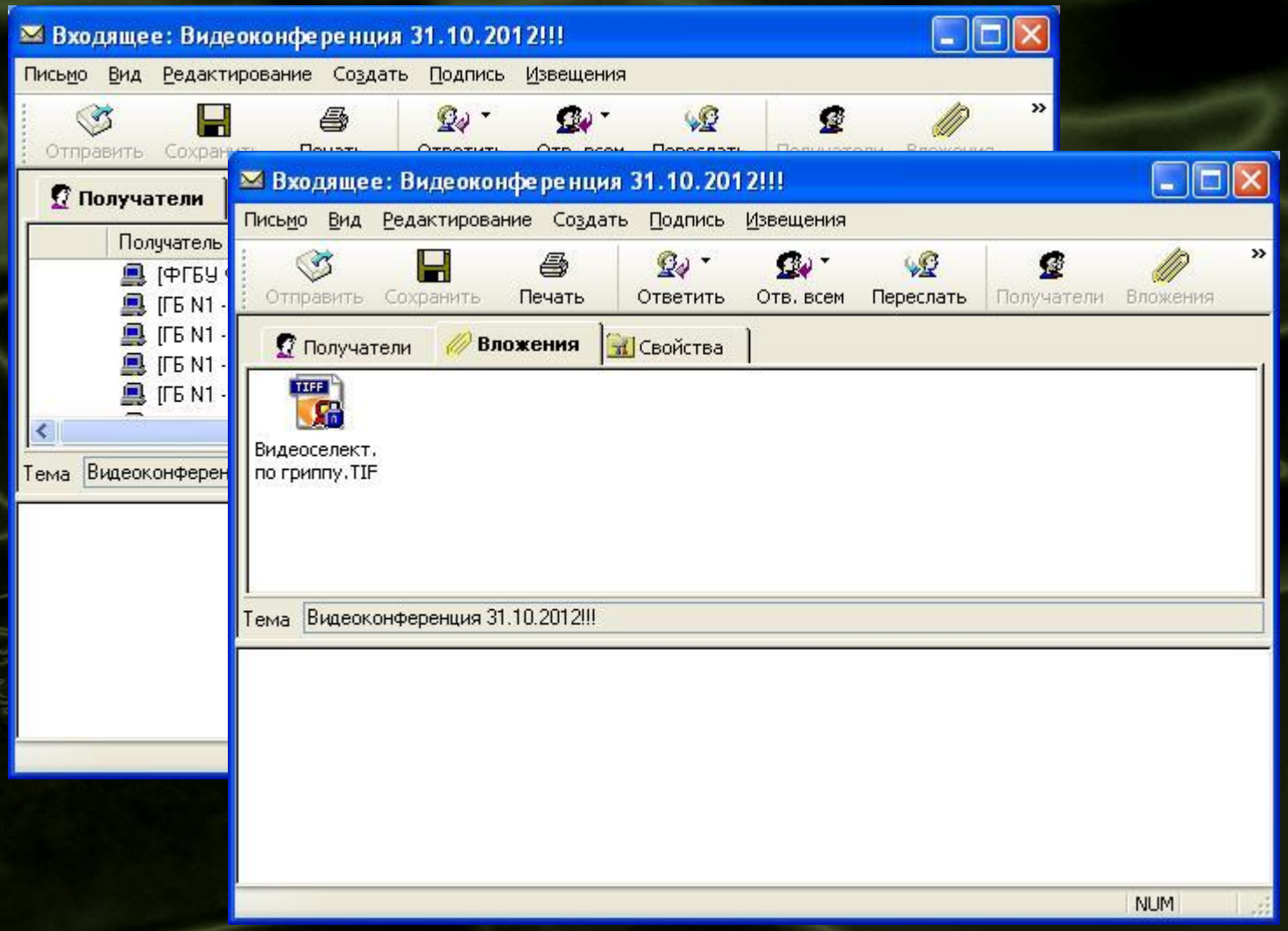
ViPNet-клиент: деловая почта



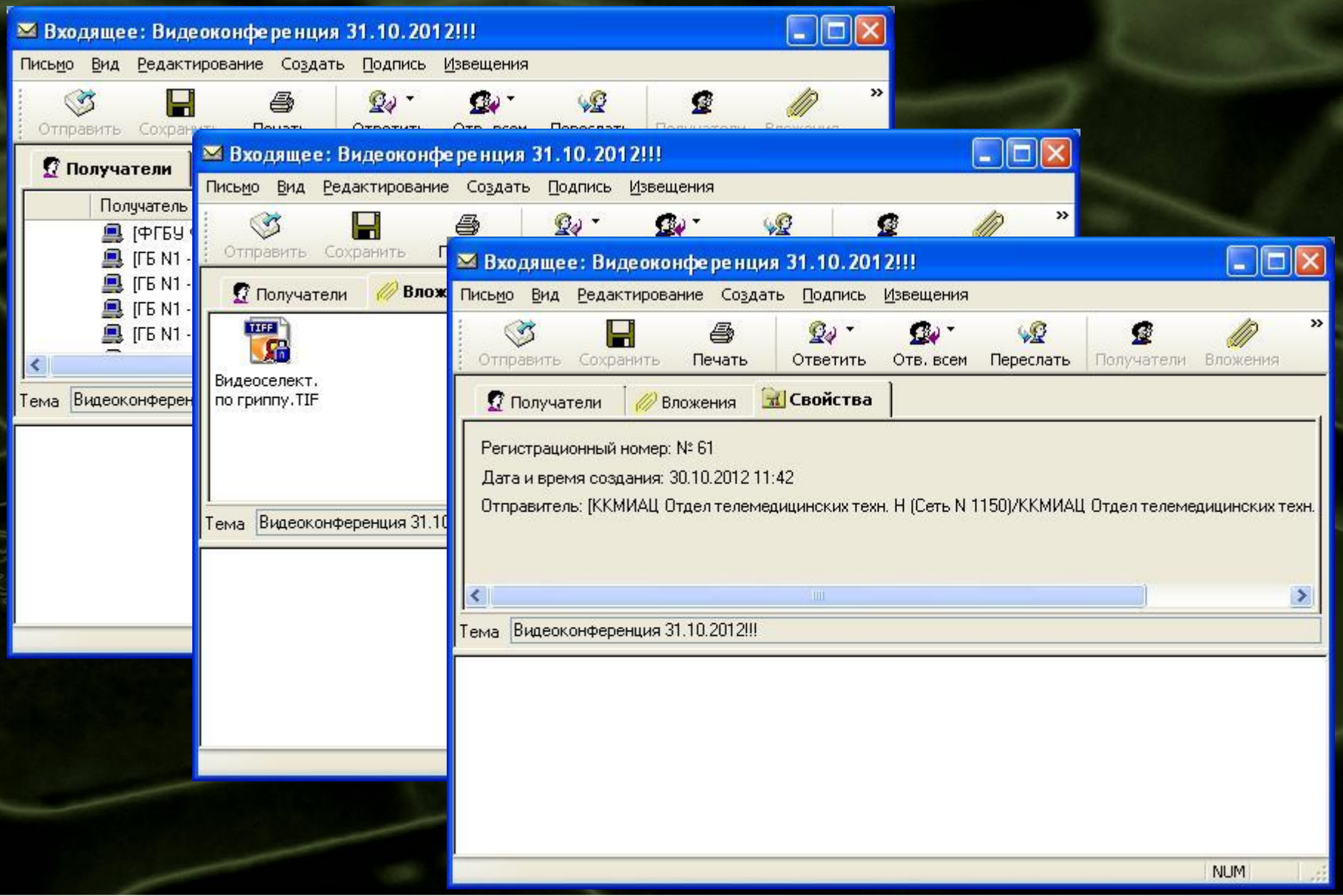
ViPNet-клиент: деловая почта

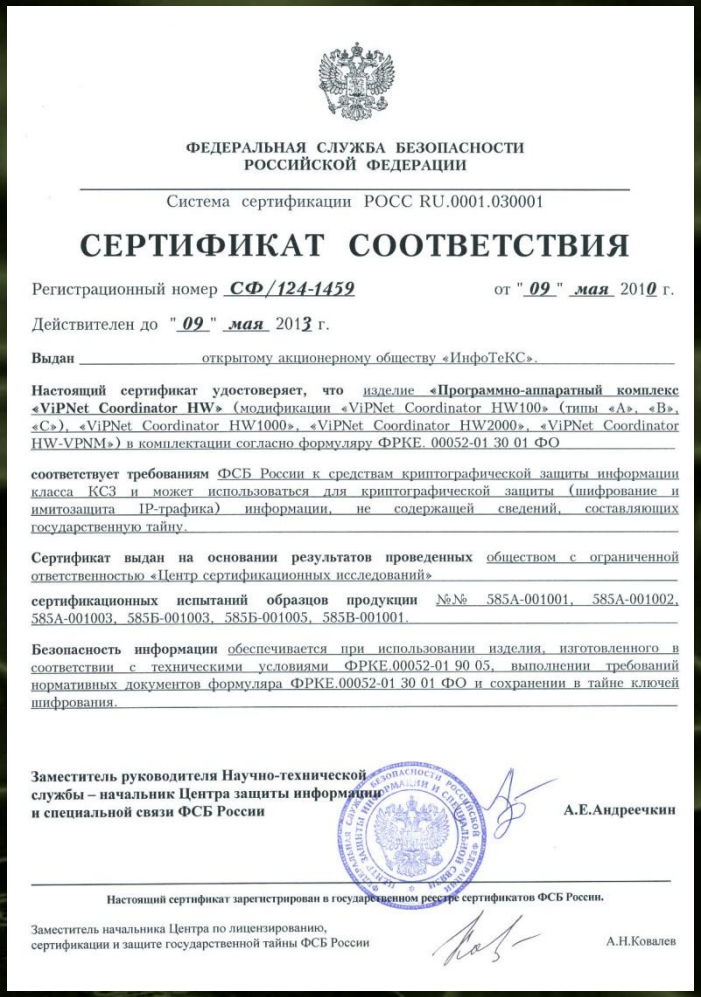


ViPNet-клиент: деловая почта



ViPNet-клиент: деловая почта





ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-1459** от "**09**" **мая** 2010 г.

Действителен до "**09**" **мая** 2013 г.

Выдан открытому акционерному обществу «ИнфоТеКС».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный комплекс «ViPNet Coordinator HW»** (модификации «ViPNet Coordinator HW100» (типы «A», «B», «C»), «ViPNet Coordinator HW1000», «ViPNet Coordinator HW2000», «ViPNet Coordinator HW-VPNM») в комплектации согласно формуляру ФРКЕ. 00052-01 30 01 ФО

соответствует требованиям ФСБ России к средствам криптографической защиты информации класса КС3 и может использоваться для криптографической защиты (шифрование и имитозащита IP-трафика) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью «Центр сертификационных исследований»

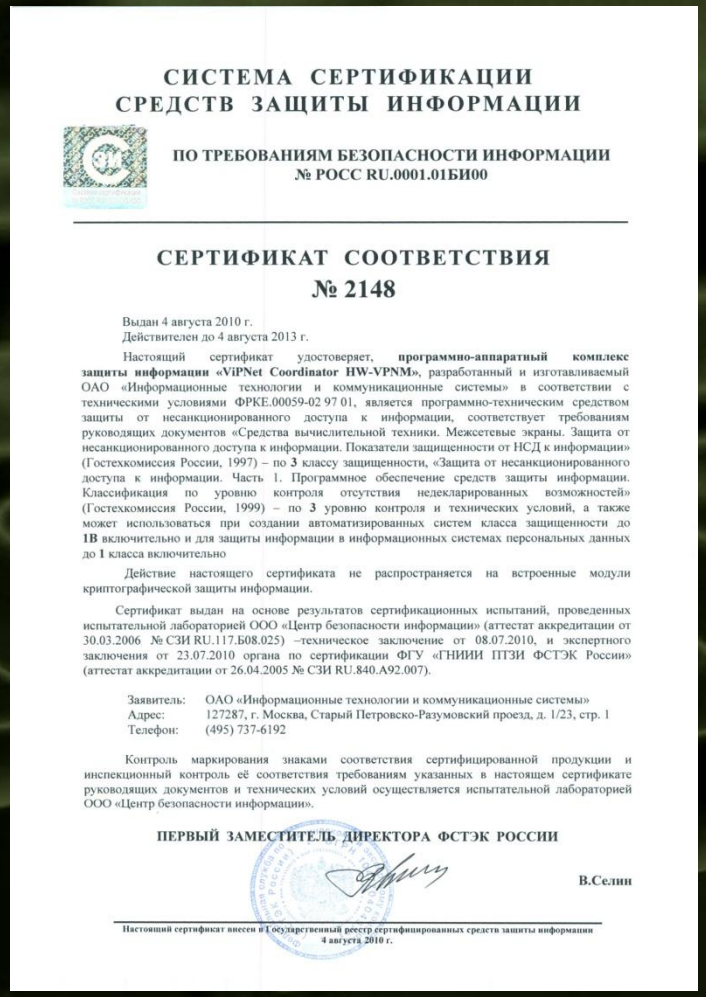
сертификационных испытаний образцов продукции №№ 585А-001001, 585А-001002, 585А-001003, 585Б-001003, 585Б-001005, 585В-001001.

Безопасность информации обеспечивается при использовании изделия, изготовленного в соответствии с техническими условиями ФРКЕ.00052-01 90 05, выполнении требований нормативных документов формуляра ФРКЕ.00052-01 30 01 ФО и сохранении в тайне ключей шифрования.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.Е.Андреечкин

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2148

Выдан 4 августа 2010 г.
Действителен до 4 августа 2013 г.

Настоящий сертификат удостоверяет, **программно-аппаратный комплекс защиты информации «ViPNet Coordinator HW-VPNM»**, разработанный и изготавливаемый ОАО «Информационные технологии и коммуникационные системы» в соответствии с техническими условиями ФРКЕ.00059-02 97 01, является программно-техническим средством защиты от несанкционированного доступа к информации, соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997) – по **3** классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по **3** уровню контроля и технических условий, а также может использоваться при создании автоматизированных систем класса защищенности до **1В** включительно и для защиты информации в информационных системах персональных данных до **1** класса включительно

Действие настоящего сертификата не распространяется на встроенные модули криптографической защиты информации.

Сертификат выдан на основе результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Центр безопасности информации» (аттестат аккредитации от 30.03.2006 № СЗИ RU.117.Б08.025) –техническое заключение от 08.07.2010, и экспертного заключения от 23.07.2010 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.A92.007).

Заявитель: ОАО «Информационные технологии и коммуникационные системы»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате руководящих документов и технических условий осуществляется испытательной лабораторией ООО «Центр безопасности информации».

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ В.Селин

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 4 августа 2010 г.

Линейка программно-аппаратных комплексов ViPNet соответствует требованиям ФСБ и ФСТЭК к СКЗИ класса КВ2 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну

Федеральные законы:

«Об электронной цифровой подписи»
№ 1-ФЗ от 10 января 2002 г.

«Об электронной подписи»
№ 63-ФЗ от 6 апреля 2011 г.

Универсальная электронная карта

Герб региона

Микропроцессор

Индивидуальный номер УЭК

Контрольный разряд

Контактные телефоны

Фото и личные данные владельца

Номер банковской карты

Логотип банка

Логотип платежной системы

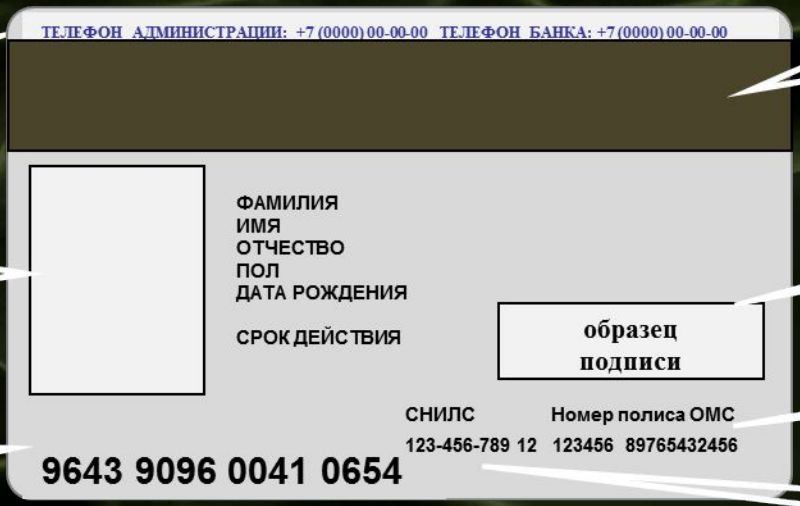
Элементы защитного комплекса

Магнитная полоса с банковским приложением

Подпись держателя карты

Номер полиса ОМС

Номер полиса ОМС



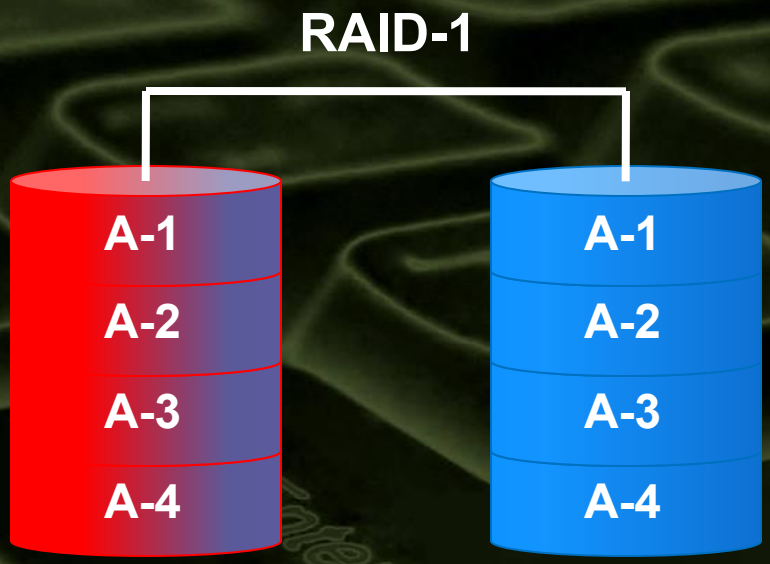
Универсальная электронная карта (УЭК)

- Физически реализуется как существующие смарт-карты с электронным чипом
- Обеспечит идентификацию гражданина при получении государственных, муниципальных и коммерческих услуг в электронном виде
- Обеспечит возможность совершения юридических действий с применением ЭЦП
- Будет являться документом, удостоверяющим личность гражданина, может использоваться как водительское удостоверение, свидетельство ИНН, полис ОМС, СНИЛС
- Обеспечит возможность получать транспортные, медицинские услуги, получать социальные начисления и пенсии, реализовать персонализированный учет льгот и дотаций
- Обеспечит использование национальной платежной системы ПРО100

Сохранность данных

- Резервирование
- Резервное копирование
- Архивирование

Резервирование:
RAID как обязательный атрибут сервера



RAID (Redundant Array of Independent Disks) —
избыточный массив независимых дисков

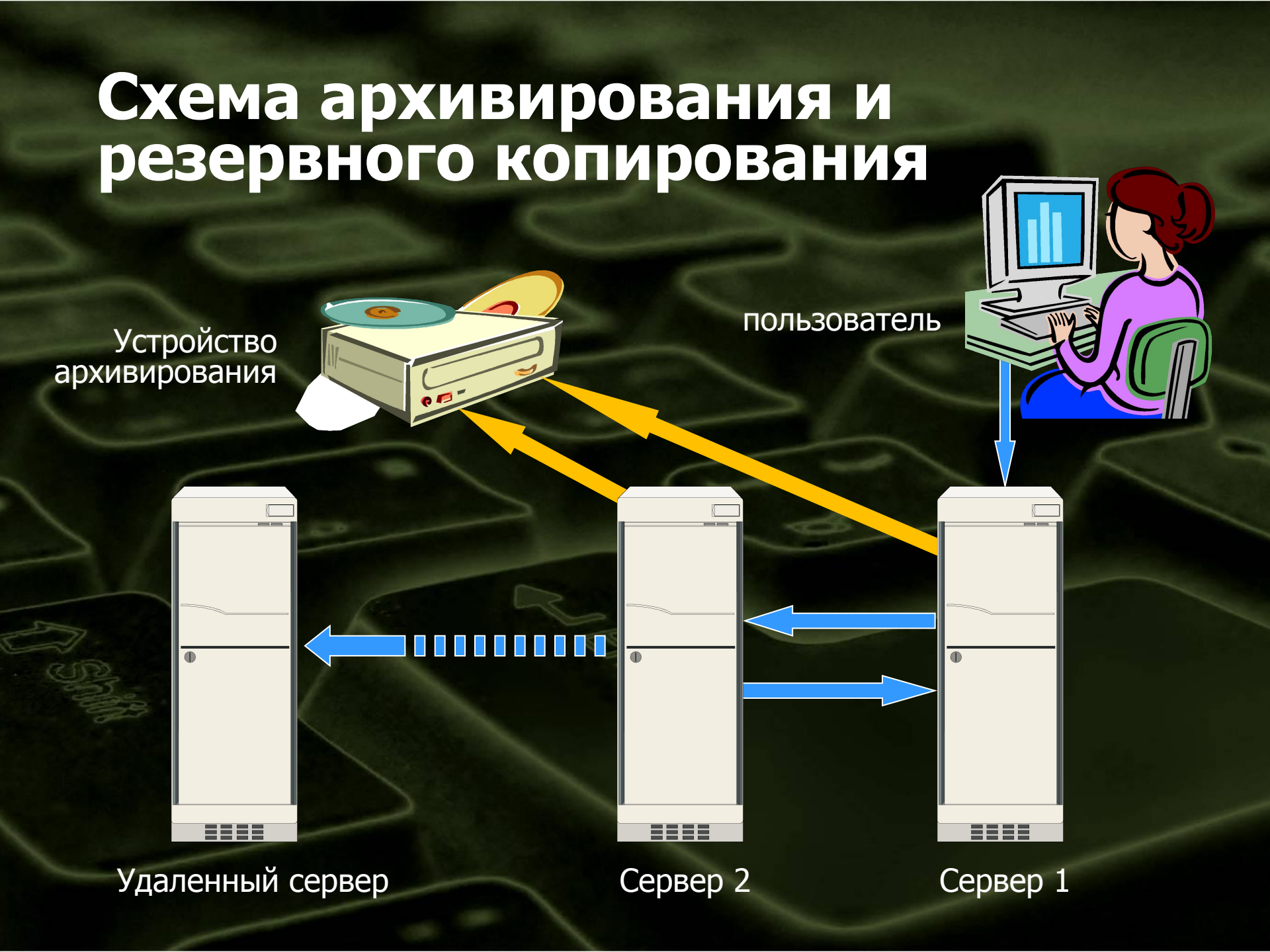
Задачи резервного копирования:

- Обеспечение сохранности возможно более свежих рабочих данных при утрате или повреждении основных носителей рабочей информации.
- Обеспечение заданной регулярности создания резервных копий.
- Обеспечение заданного времени восстановления рабочей информации из резервной копии

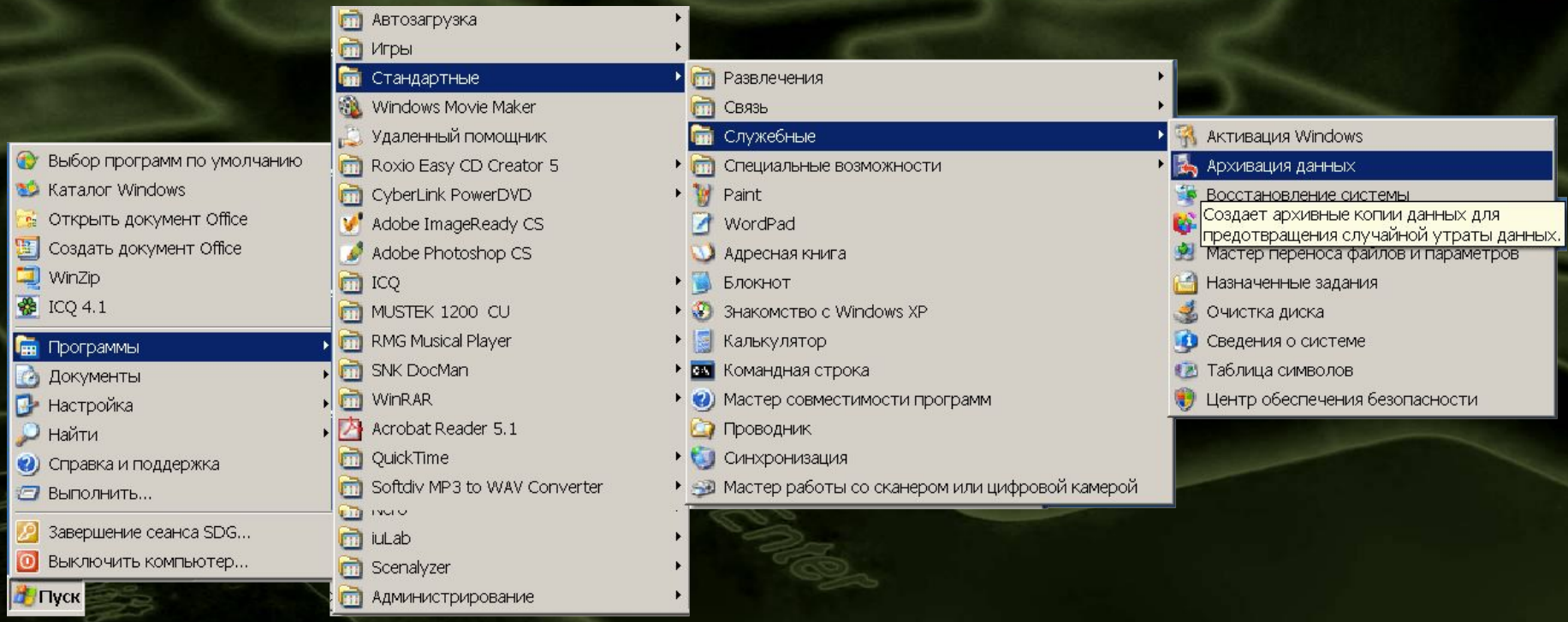
Задачи архивирования:

- Обеспечение возможности просмотра старых версий файлов, в том числе файлов, уже удаленных с серверов локальной сети.
- Обеспечение надежного хранение архивных данных в течение установленного периода времени.
- Обеспечение заданного времени доступа к запрошенной архивной или рабочей информации.

Схема архивирования и резервного копирования

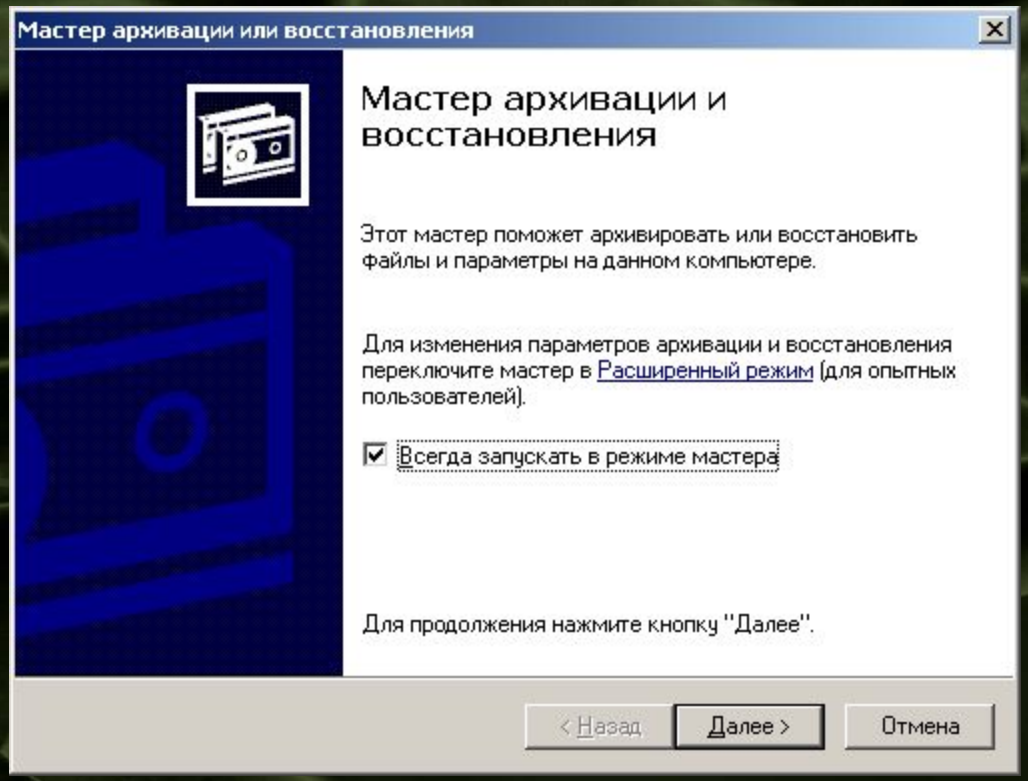


Запуск мастера архивации и восстановления



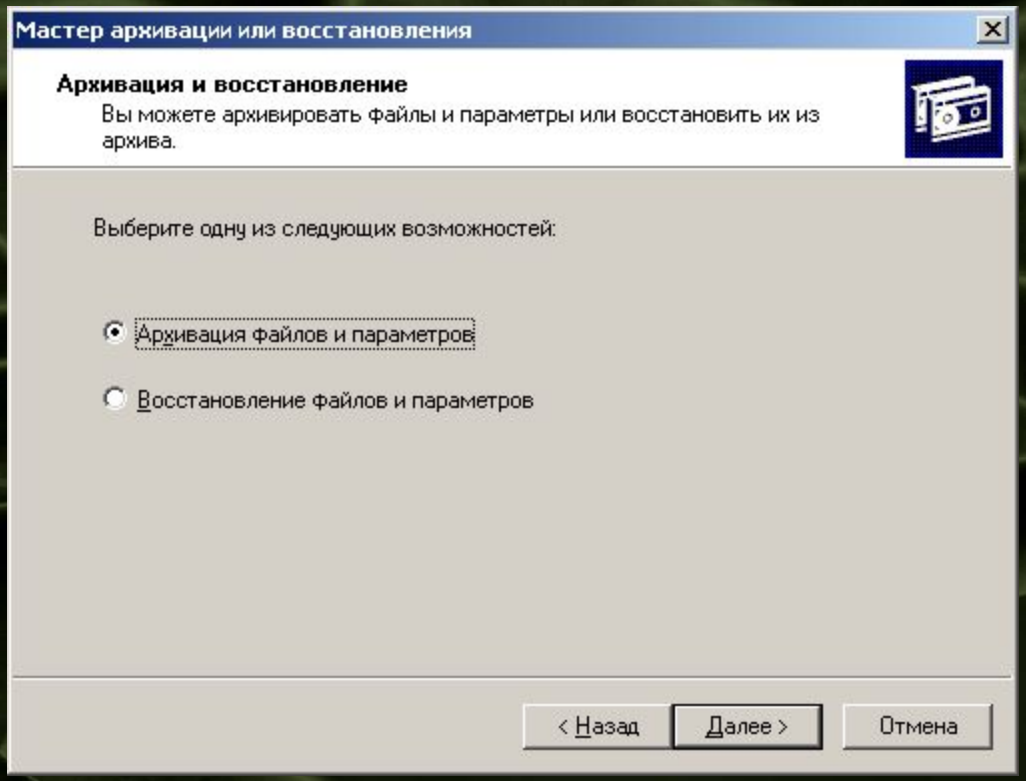
Пуск > Программы > Стандартные > Служебные > Архивация данных

Настройка архивации данных



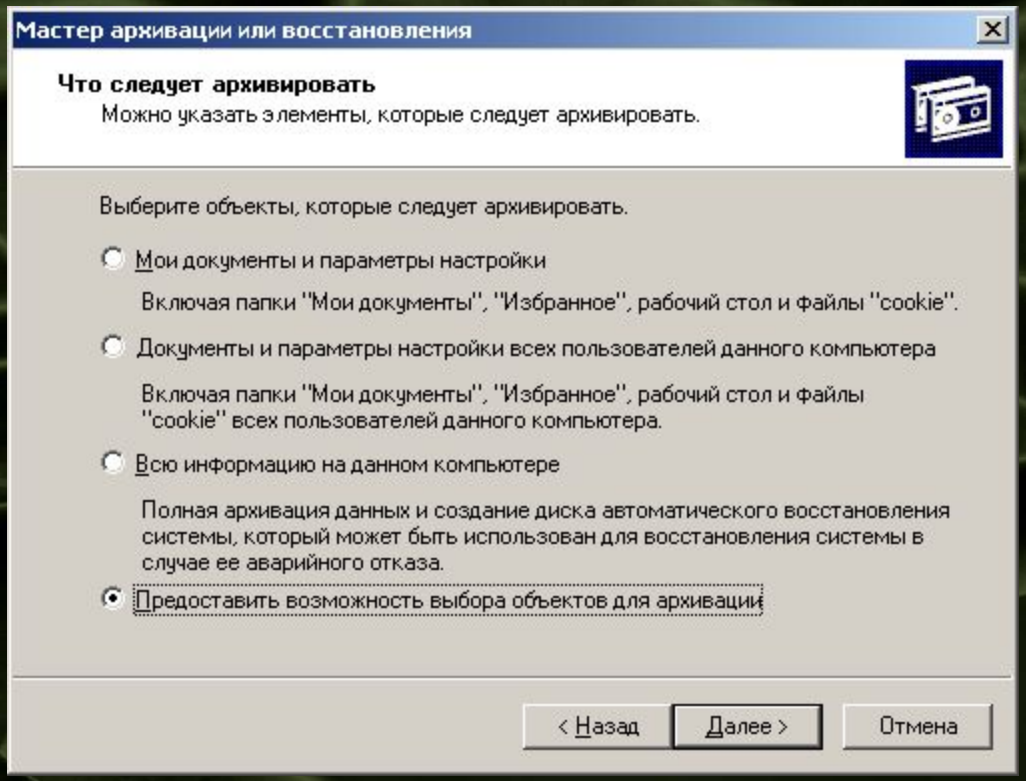
Шаг 1

Настройка архивации данных



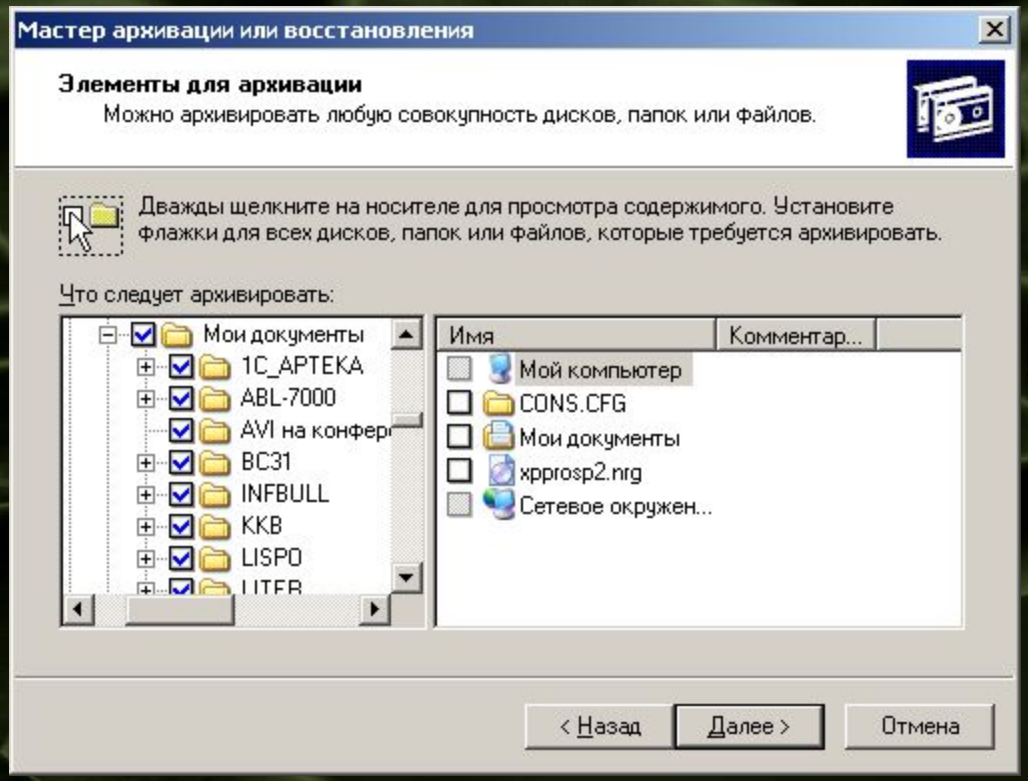
Шаг 2

Настройка архивации данных



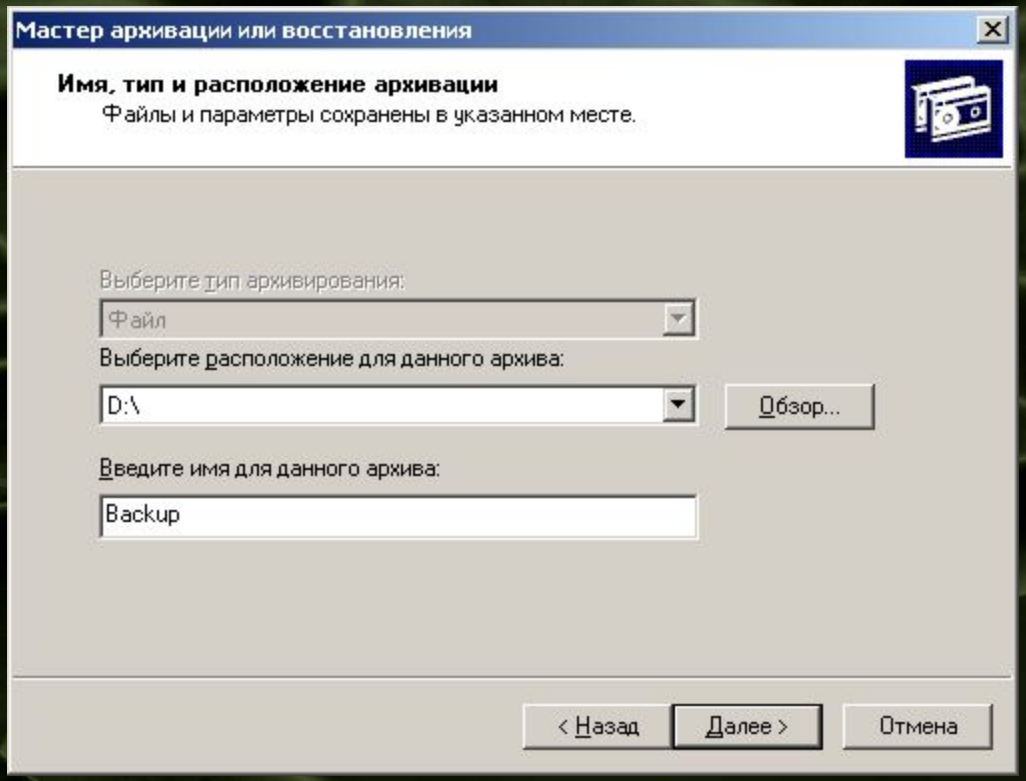
Шаг 3

Настройка архивации данных



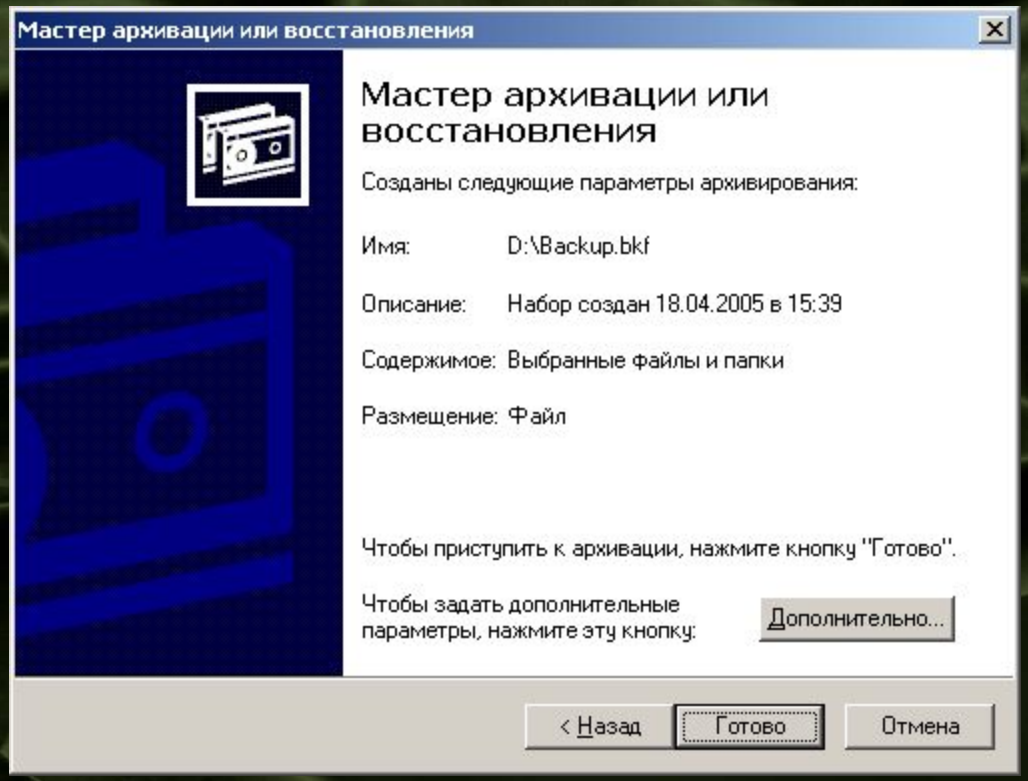
Шаг 4

Настройка архивации данных



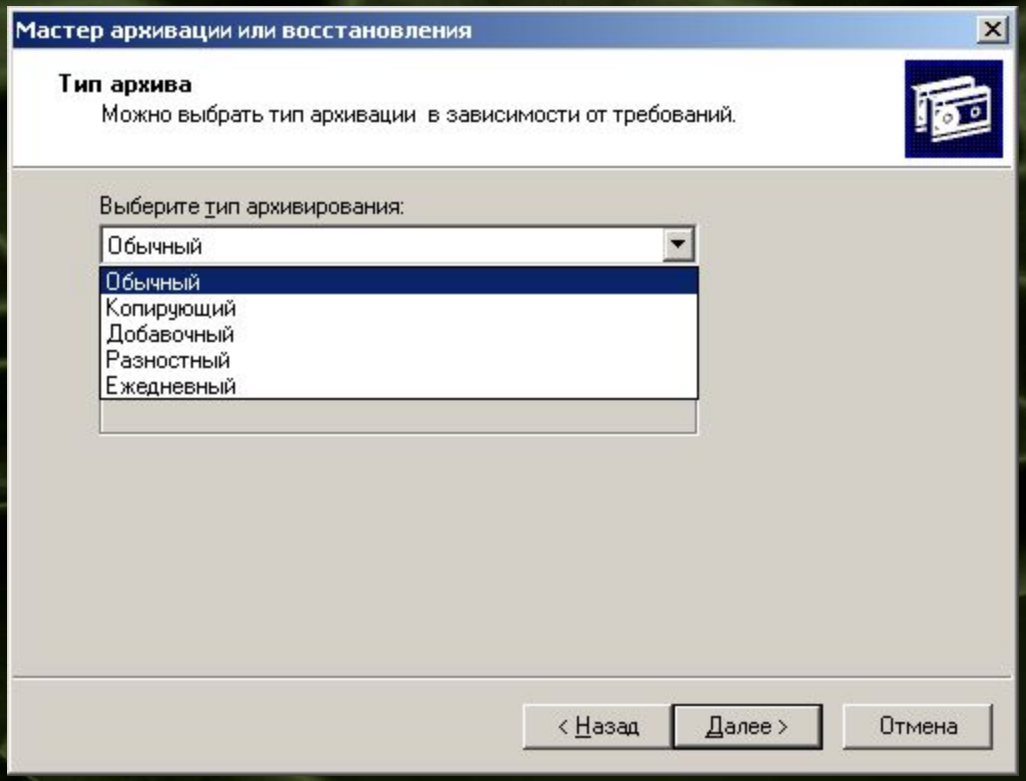
Шаг 5

Настройка архивации данных



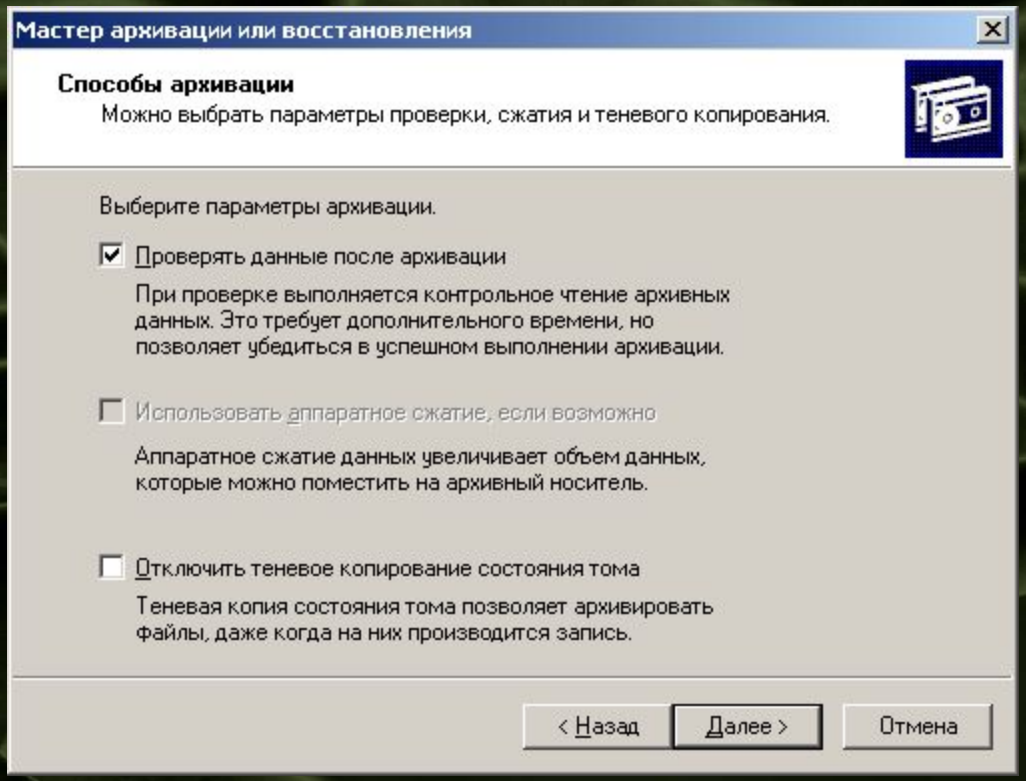
Шаг 6

Настройка архивации данных



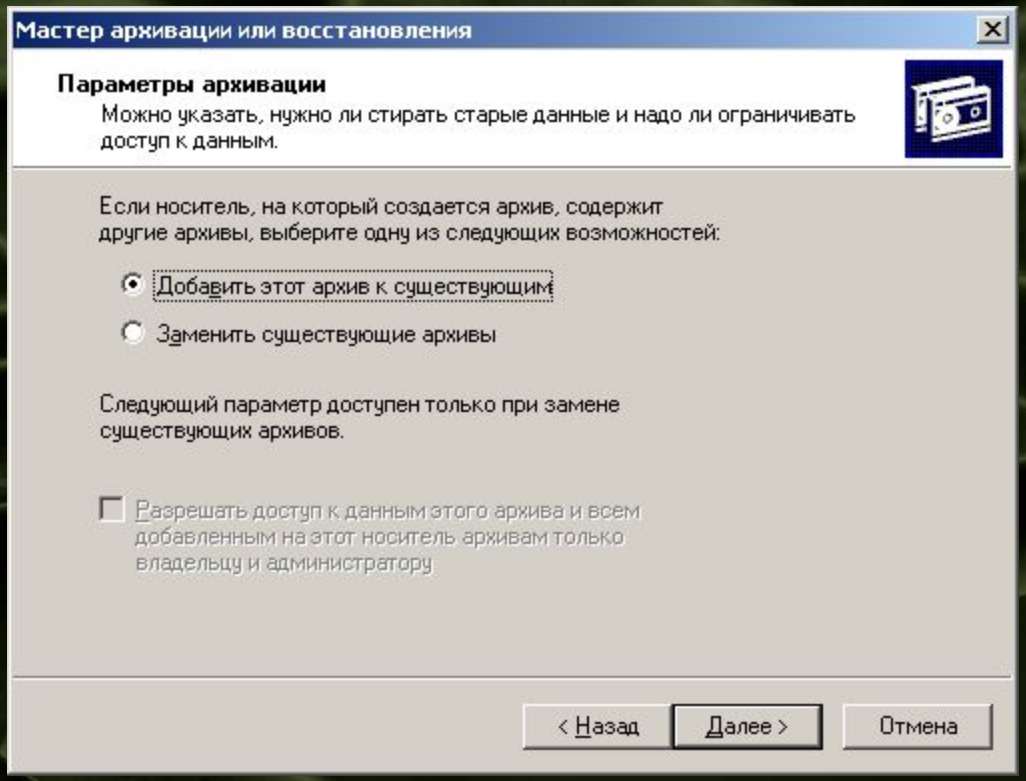
Шаг 7

Настройка архивации данных



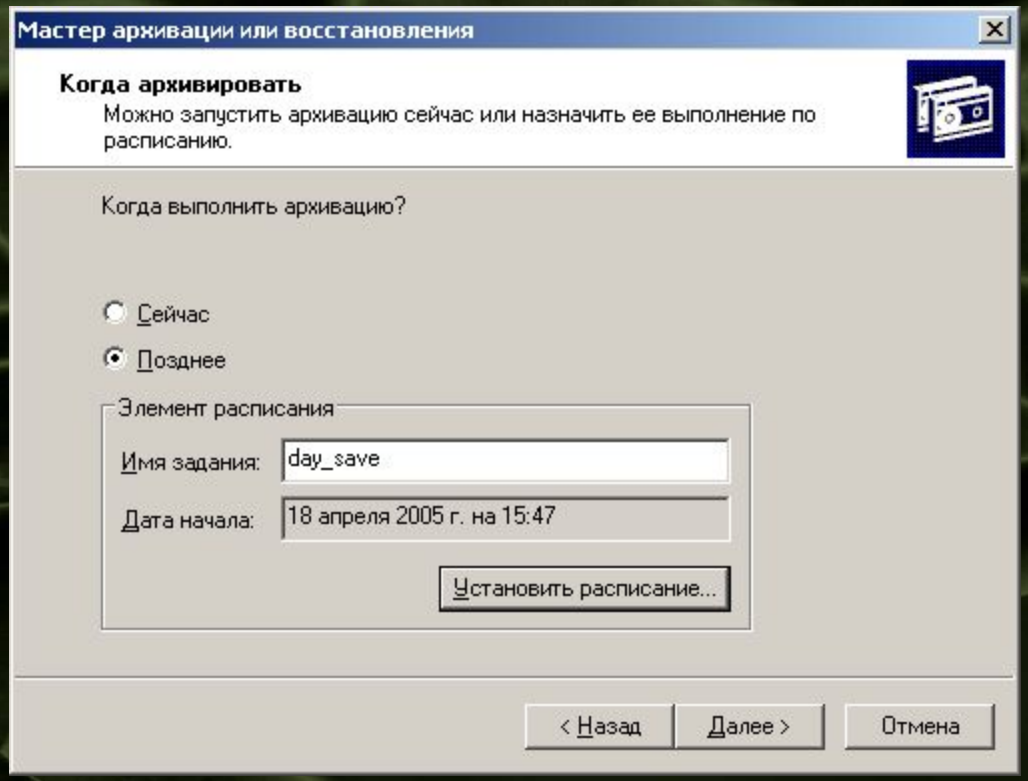
Шаг 8

Настройка архивации данных



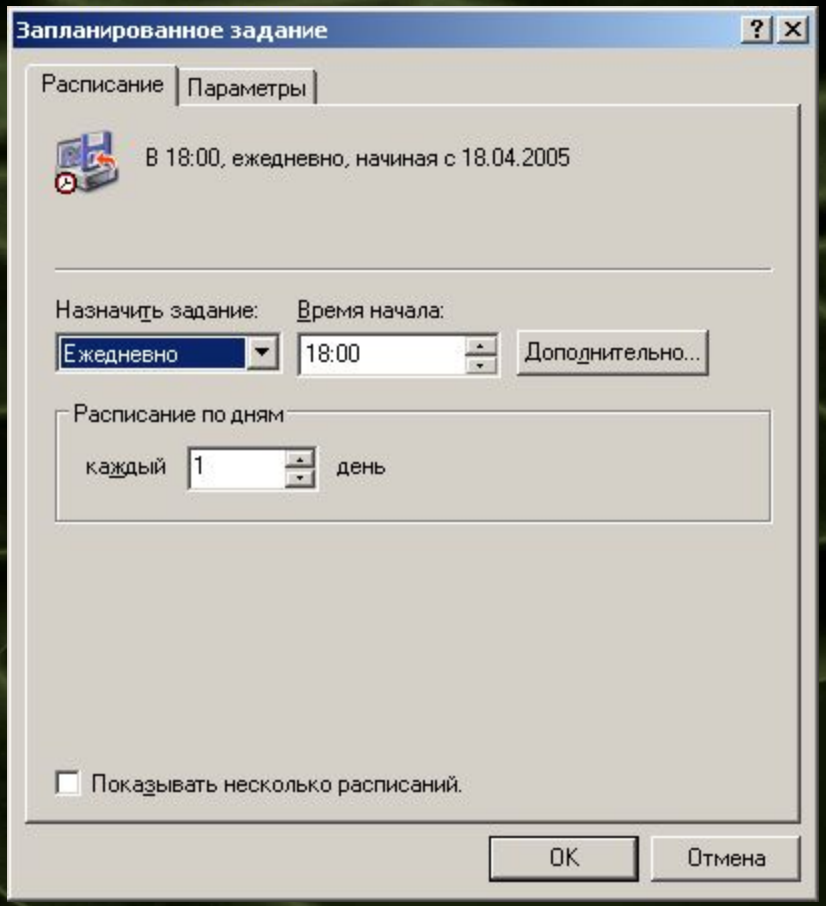
Шаг 9

Настройка архивации данных



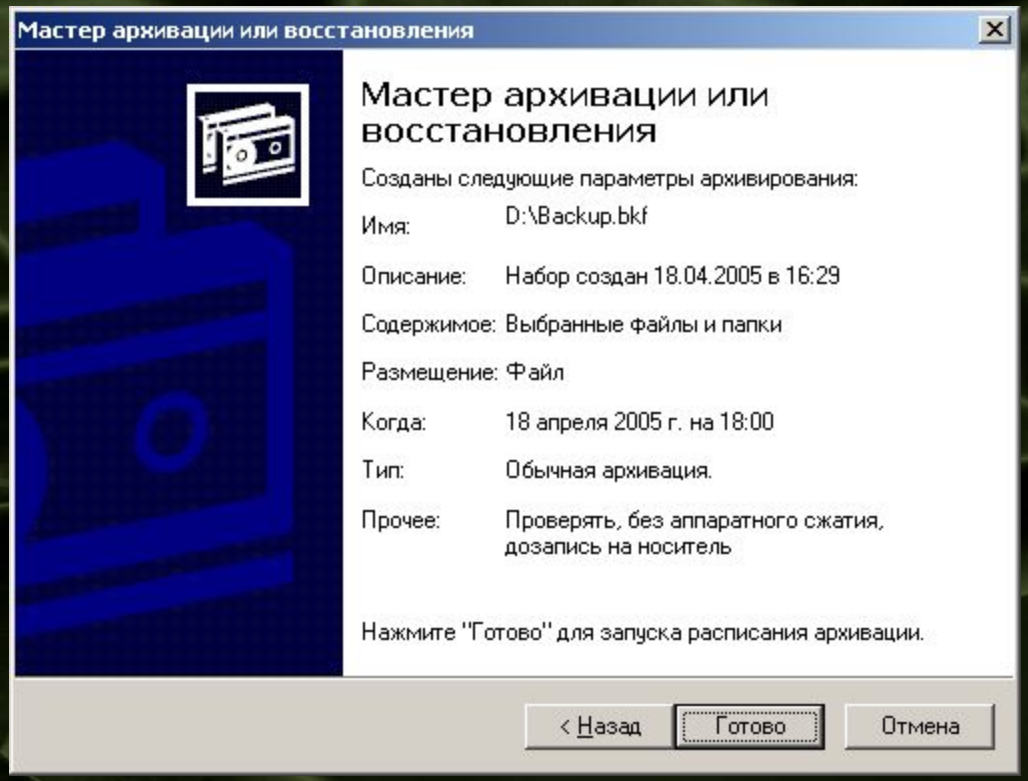
Шаг 10

Настройка архивации данных

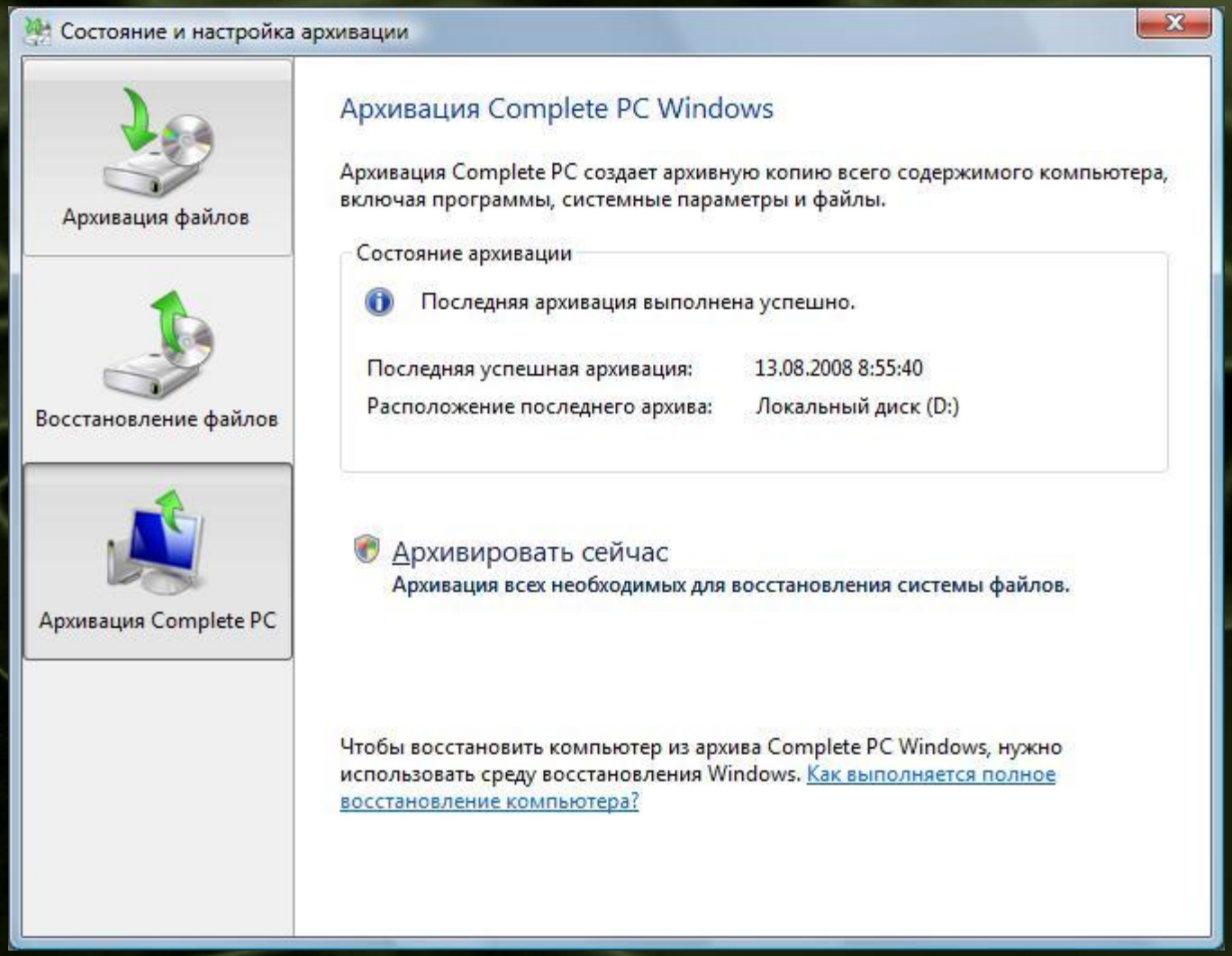


Шаг 11

Настройка архивации данных



Шаг 12


Состояние и настройка архивации
Архивация файлов
Восстановление файлов
Архивация Complete PC
Архивация Complete PC Windows
Архивация Complete PC создает архивную копию всего содержимого компьютера, включая программы, системные параметры и файлы.
Состояние архивации
Последняя архивация выполнена успешно.
Последняя успешная архивация: 13.08.2008 8:55:40
Расположение последнего архива: Локальный диск (D:)
Архивировать сейчас
Архивация всех необходимых для восстановления системы файлов.
Чтобы восстановить компьютер из архива Complete PC Windows, нужно использовать среду восстановления Windows. Как выполняется полное восстановление компьютера?

Надежность информационной системы

- **Готовность к использованию** (система доступна для взаимодействия и применения);
- **Безопасность** (система имеет средства защиты от несанкционированного физического и логического доступа);
- **Целостность** (функционирование системы характеризуется полнотой, точностью, своевременностью и санкционированностью);
- **Сопровождаемость** (при необходимости система может подвергаться модернизации таким образом, что при последующем использовании она продолжает обладать тремя предыдущими свойствами).

“Доверие к системам. Принципы и критерии надежности систем. Версия 2.0”
(SysTrust (SM/TM). Principes and Criteria for Systems Reliability. Version 2.0).

Информационная безопасность и локальные вычислительные сети

- Использование ЛВС с контроллером домена, управляющим всей работой сети, сертифицированным Гостехкомиссией
- Установка и настройка операционных систем на компьютерах пользователей сетевым администратором или его помощником
- Запрещение внесения каких-либо изменений в сетевые настройки со стороны пользователей
- Запрещение разрешения общего доступа к дискам и папкам компьютера
- Доступ к ресурсам компьютера должен разрешаться лишь конкретным пользователям
- Запрещение пользователям самостоятельной установки какого – либо программного обеспечения
- Все рабочие станции должны иметь резидентные антивирусные программы

Защита информации от пользователя

- Несоблюдение процедуры выхода из системы (выключения компьютера)
- Подключение компьютера к электрической сети, параллельно с бытовыми приборами (холодильниками, электрическими нагревателями и пр.), являющимися причиной бросков напряжения и выхода компьютера из строя; отсутствие сетевых фильтров и источников бесперебойного питания
- Несвоевременное обнаружение отказа вентиляторов источника питания, процессора, видеокарты
- Невыполнение проверок жесткого диска на наличие логических и физических ошибок, удаления временных файлов и дефрагментации
- Игнорирование системных сообщений об обнаруженных ошибках
- Неиспользование антивирусных программ или несвоевременное обновление их баз данных

Защита информации от пользователя

- Обучение пользователей;
- Разработка четких инструкций и требований по работе с программно – аппаратными средствами с указанием мер ответственности за их нарушение;
- Контроль за их исполнением и применение к нарушителям реальных и ощутимых санкций.

Опасности «глобализации»

Опасности «глобализации»

2 ноября 1988 года выпускник Корнельского университета Роберт Таппан Моррис запустил свою программу, которая вышла из-под контроля автора и начала быстро перемещаться по сети.

Червь Морриса инфицировал 6200 компьютеров.
К прямым потерям были отнесены:

- остановка, тестирование и перезагрузка 42700 машин;
- идентификация червя, удаление, чистка памяти и восстановление работоспособности 6200 машин;
- анализ кода червя, дизассемблирование и документирование;
- исправление UNIX систем и тестирование.

Прямые потери были оценены более чем в 32 000 000 долларов.
К косвенным потерям были отнесены:

- потери машинного времени в результате отсутствия доступа к сети;
- потери доступа пользователей к сети.

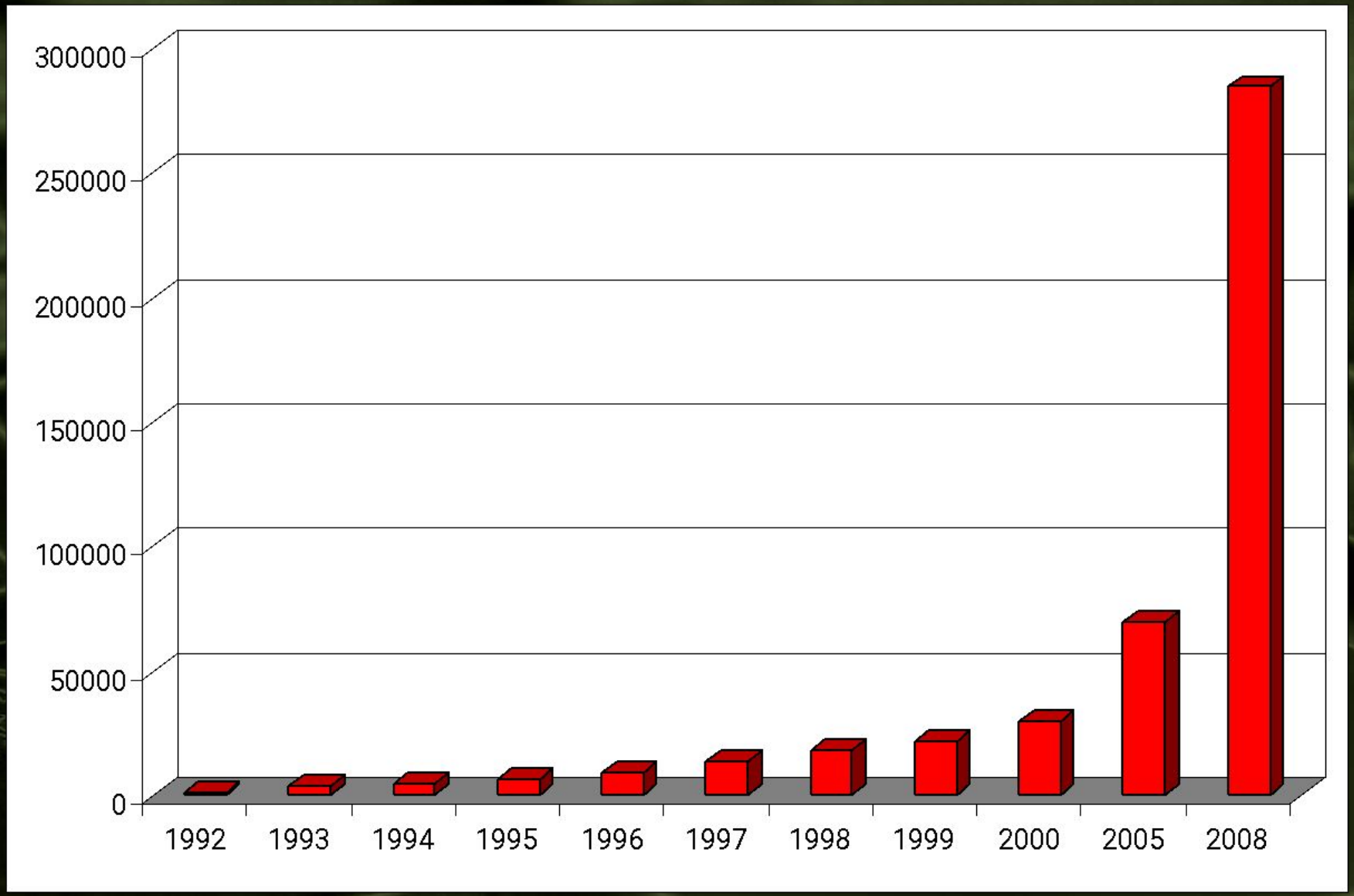
Косвенные потери были оценены более чем в 66 000 000 долларов.
Общие затраты были оценены на сумму в 98 253 260 долларов

Системы групповой работы и обмена сообщения являются легкой добычей для вредоносного кода и распространения нежелательного содержимого:

- Вирусы
- Вирусы-черви
- Программы «Троянские кони»
- Root-kits, bot-nets
- Нежелательные сообщения
- Фишинг
- Оскорбления и унижения

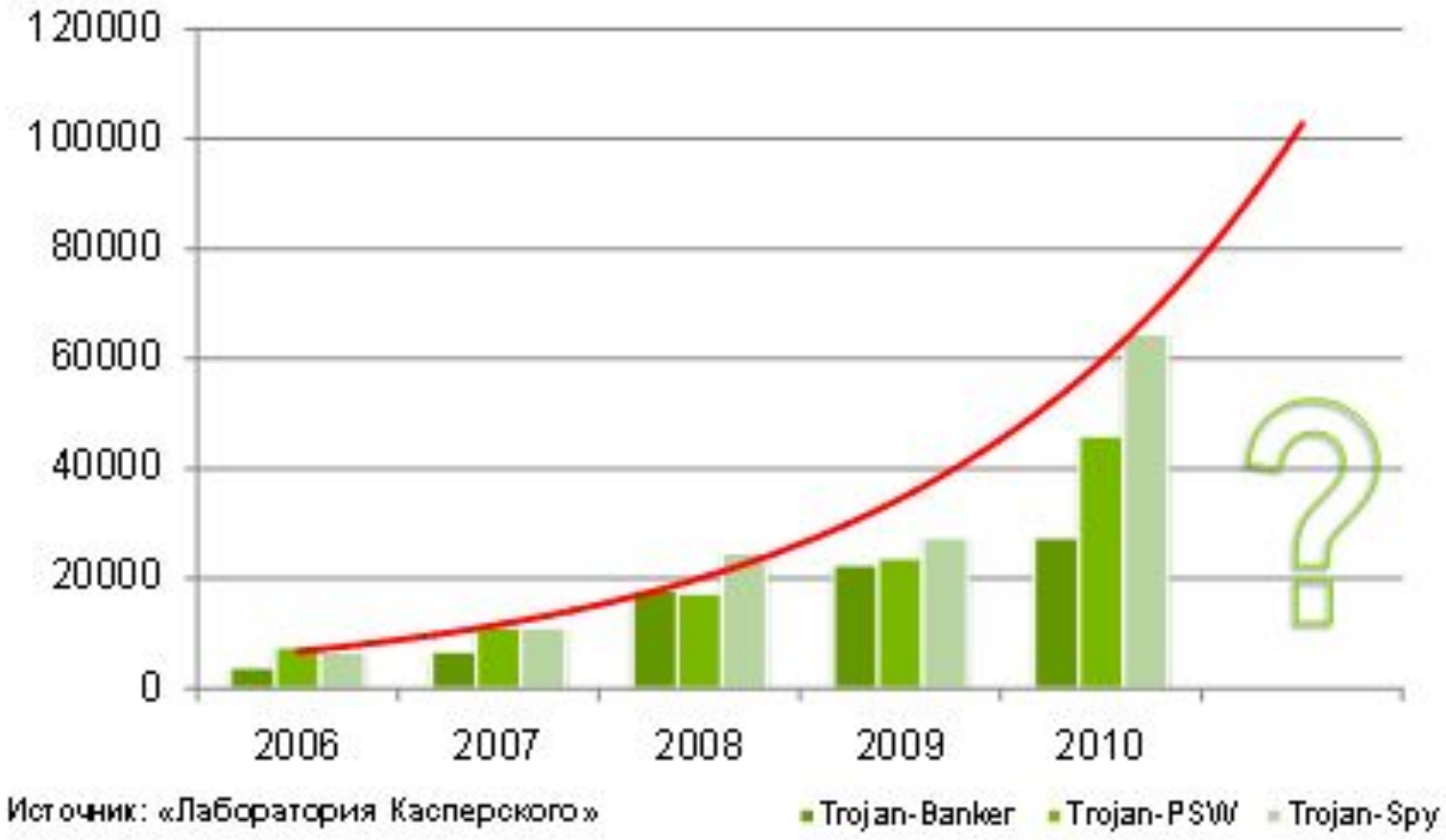
Опасности «глобализации»

- В августе 1996 года атакован сервер департамента юстиции США. В течение нескольких часов страницы сервера были заполнены фашистской атрибутикой и содержали пародию на Билль о телекоммуникациях.
- 6 сентября 1996 года атаке подвергся сервер компании PANIX, являющейся одним из крупнейших провайдеров Internet. В результате атаки компания несколько дней не могла предоставлять услуги своим абонентам.
- В октябре 1996 года на сервере ЦРУ вместо "Welcome to the Central Intelligent Agency" появился заголовок "Welcome to the Central Stupidity Agency" и непристойные тексты.
- 5 ноября 1996 года был атакован WWW-сервер газеты Нью-Йорк Таймс, в результате чего было практически невозможно следить за ходом президентских выборов.
- В ноябре 1996 года румынские кракеры заменили на WWW-сервере правительства портрет президента Илиеску на портрет его соперника Константинеску.
- 5 марта 1997 года взломан сервер NASA в Центре управления космическими полетами Годдарда. Кракеры разместили на страницах сервера свое обращение, в котором осуждалась коммерциализация Internet и выражался протест против судебного преследования знаменитых взломщиков Кевина Митника и Эда Каммингса..
- 20 марта был вскрыт сервер Сэнфорда Уоллейса – президента рекламной фирмы Cyber Promotions. Кракеры поместили в UseNet копию похищенного файла паролей, содержащего зашифрованные пароли, имена и телефоны клиентов фирмы.



Число компьютерных вирусов за последние 15 лет

Динамика роста объемов вредоносного ПО, предназначенного для кражи информации



Источник: «Лаборатория Касперского»

Антивирусная защита

- Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам от сторонних лиц и организаций;
- При возникновении подозрения на наличие компьютерного вируса пользователь должен провести внеочередной антивирусный контроль, или при необходимости привлечь специалистов информационного подразделения для определения факта наличия или отсутствия компьютерного вируса;
- При обнаружении компьютерного вируса пользователь или сетевой администратор обязан приостановить работу, провести лечение заражённых вирусом файлов штатными антивирусными средствами, а при невозможности или неэффективности лечения уничтожить заражённые вирусом файлы способом, исключающим их восстановление.

- Ядра, разработанные различными лабораториями, имеют различный уровень эвристики
- У каждой лаборатории свой цикл выпуска обновлений вирусных сигнатур

	Количество обновлений в день
Kaspersky	20
Panda	7
F-Secure	6 - 7
Dr. Web	6
AntiVir, H+BEDV	5 - 6
eSafe	5
Computer Associates	4 - 5
F-Prot	4 - 5
Sophos	4 – 5
Trend Micro	2 – 3
Symantec	1 - 2

AV-Test.org 2004

http://www.av-test.org/down/papers/2004-02_vb_outbreak.pdf

Опасности «глобализации»

- Все программы, используемые для доступа в Интернет, должны быть утверждены сетевым администратором и на них должны быть установлены все доработки производителя (patch), связанные с безопасностью.
- Во всех браузерах должно быть запрещена обработка Java, JavaScript и ActiveX из-за небезопасности данных технологий.
- Все браузеры должны быть сконфигурированы так, чтобы для доступа в Интернет использовался прокси-сервер из состава брандмауэра.
- Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, должны быть запротоколированы, и использоваться для принятия решения о применении к нему санкций административного характера.

Опасности «глобализации»

- Пересылка сообщений, содержащих конфиденциальную информацию, допускается лишь при использовании лицензированных средств криптографической защиты.
- Для пересылки служебной информации запрещается использовать свои и чужие почтовые ящики, открытые на общедоступных почтовых серверах (Mail.ru, Rambler.ru и пр.).

Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

Об информации, информационных технологиях и о защите информации
Федеральный Закон № 149-ФЗ
от 27 июля 2006 года Статья 17. п. 1

Применение санкций за несоблюдение требований информационной безопасности возможно, если:

- **Информация имеет действительную или потенциальную коммерческую ценность,**
- **Учреждение принимает определенные меры по охране конфиденциальности,**
- **Все сотрудники, знакомые с этими сведениями, должны быть официально предупреждены об их конфиденциальности.**

статья 139 Гражданского кодекса Российской Федерации

Дисциплинарные взыскания

определены Трудовым кодексом РФ
от 30 декабря 2001 г. № 197-ФЗ.

За совершение дисциплинарного проступка, т.е. неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:
замечание, выговор, увольнение по соответствующим основаниям.

Федеральными законами, уставами и положениями о дисциплине для отдельных категорий работников могут быть предусмотрены также и другие дисциплинарные взыскания. Порядок их применения сформулирован в ст. 193 Трудового кодекса РФ.

Дисциплинарное взыскание применяется не позднее одного месяца со дня обнаружения проступка, не считая времени болезни работника, пребывания его в отпуске, а также времени, необходимого на учет мнения представительного органа работников.

Дисциплинарные взыскания

определены Трудовым кодексом РФ
от 30 декабря 2001 г. № 197-ФЗ.

За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.
Приказ (распоряжение) работодателя о его применении объявляется работнику под роспись в течение трех рабочих дней со дня его издания, не считая времени отсутствия работника на работе.
Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим его.
Работодатель до истечения года со дня применения дисциплинарного взыскания имеет право снять его с работника по собственной инициативе, просьбе самого работника, ходатайству его непосредственного руководителя или представительного органа работников.

Административным правонарушением

признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое Кодексом или законами субъектов РФ об административных правонарушениях установлена административная ответственность в виде штрафа, который является денежным взысканием и может выражаться в величине, кратной:

- минимальному размеру оплаты труда (без учета районных коэффициентов), установленному федеральным законом на момент окончания или пресечения административного правонарушения;
- стоимости предмета административного правонарушения на момент окончания или пресечения административного правонарушения.

Размер административного штрафа, налагаемого
на граждан, не может превышать двадцать пять
минимальных размеров оплаты труда
(МРОТ),
на должностных лиц – пятьдесят МРОТ,
на юридических лиц – одну тысячу МРОТ.

Кодекс РФ об административных правонарушениях устанавливает меру ответственности за нарушения законодательства в области связи и информации.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа

на граждан в размере от пяти до десяти МРОТ с конфискацией несертифицированных средств защиты информации или без таковой;

на должностных лиц - от десяти до двадцати МРОТ;

на юридических лиц - от ста до двухсот МРОТ с конфискацией несертифицированных средств защиты информации или без таковой.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб* или совершенное из корыстной заинтересованности, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

* - крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 272. Неправомерный доступ к компьютерной информации

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, –

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия* или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет

* – тяжкие последствия – приносящие вред здоровью или смерть человека (в зависимости от контекста статьи УК)

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, –

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

ПРО ЭТО НУЖНО ПОМНИТЬ !