

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Дини Ирина Анатольевна

Должность: Декан факультета лингвистики

Дата подписания: 19.10.2020 19:31:05

Уникальный программный ключ:

dbded7a521afad7b173f5356b48fe0e97c4d89a005059664244ac4be5f49e53d



**Образовательное частное учреждение
высшего образования «Институт международного права и
экономики имени А. С. Грибоедова»**

Кафедра гуманитарно-педагогических и естественнонаучных дисциплин

УТВЕРЖДАЮ:

Декан факультета лингвистики

_____/И.А. Дини/

«28» октября 2020 г

Рабочая программа дисциплины

Основы информационной безопасности в профессиональной деятельности

Укрупненная группа специальностей 45.00.00

**Специальность 45.05.01 Перевод и переводоведение
(уровень специалитета)**

**Специализация: «Лингвистическое обеспечение
межгосударственных отношений»**

Форма обучения: очная

Москва

Рабочая программа дисциплины «Основы информационной безопасности в профессиональной деятельности». Специальность 45.05.01 Перевод и переводоведение / сост. А.С. Скотченко– М.: ИМПЭ им. А.С. Грибоедова, 2019. – 48 с.

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по специальности 45.05.01 «Перевод и переводоведение», утвержденного приказом Министерства образования и науки Российской Федерации от 17 октября 2016 г. № 1290.

Разработчики: к.т.н., доцент А.С. Скотченко

Ответственный рецензент: канд.филол.наук, доц., декан факультета иностранных языков ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого» Д.А. Разоренов

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры лингвистики и переводоведения от 28 октября 2020 г. N2.

И.о. заведующего кафедрой _____ /Н.В. Автионова/

Согласовано от Библиотеки _____ /О.Е. Степкина/

Согласовано от Работодателей:

Ассоциация гидов-переводчиков, экскурсоводов и турменеджеров _____ /Генеральный директор Е.В. Тихонова/

АНО ДПО «Гуманитарный институт» _____ /Директор Т.С. Круглова /

Раздел 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи дисциплины конкретизируют сформулированную общую цель и способствуют ее реализации:

- приобретение информационной культуры;
- владение методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей;
- способность понимать сущность и значение информации в развитии современного информационного общества, соблюдать основные требования информационной безопасности;
- способность распознавания опасности и угроз, возникающих в процессе использования информации и применения основных способов защиты от внешних и внутренних угроз.

Раздел 2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Основы информационной безопасности в профессиональной деятельности» направлен на формирование следующих компетенций, которые позволят усваивать теоретический материал учебной дисциплины и реализовывать практические задачи (таблица 2.1) и достигать планируемые результаты обучения по дисциплине.

Таблица 2.1

Компетентностная карта дисциплины

Индекс по ФГОС ВО	Содержание компетенции	Планируемые результаты обучения по дисциплине (модулю): (знания, умения, навыки)
ОПК-1	способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке	Знать: технологии работы с различными источниками информации Уметь: осуществлять поиск, хранение, обработку и анализ информации из разных источников Владеть: стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке
ОПК-5	способностью самостоятельно	Знать: методику работы с источниками

	осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных	информации Уметь: самостоятельно осуществлять поиск и подбор информации Владеть: навыками оценки и анализа информации
--	---	---

Раздел 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности в профессиональной деятельности» входит в состав базовой части блока 1 «Дисциплины» (модули) основной профессиональной образовательной программы специалиста по направлению подготовки 45.05.01 Перевод и переводоведение. Дисциплина призвана углубить знания обучающихся в области информационных технологий и их практического применения.

К исходным требованиям, необходимым для изучения дисциплины, относятся знания, умения и компетенции, сформированные у обучающихся в средней общеобразовательной школе и в процессе изучения дисциплины «Информатика».

Дисциплина «Основы информационной безопасности в профессиональной деятельности» является основой для изучения всех дисциплин профессиональной подготовки, для прохождения производственной практики, а также для осуществления научно-исследовательской деятельности обучающихся при написании курсовой и выпускной квалификационной работ.

Раздел 4. ОБЪЕМ (ТРУДОЕМКОСТЬ) ДИСЦИПЛИНЫ (ОБЩАЯ, ПО ВИДАМ УЧЕБНОЙ РАБОТЫ, ВИДАМ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ)

Таблица 4.1

Трудоёмкость дисциплины и виды учебной работы на очной форме обучения

Структура и содержание дисциплины

**Перечень разделов (модулей), тем дисциплины и
распределение учебного времени по разделам\темам дисциплины, видам учебных
занятий (в т.ч. контактной работы), видам текущего контроля**

Таблица 4.2

Распределение учебной нагрузки по разделам дисциплины на очной форме обучения

Темы\разделы (модули)	Контактная работа				Часы СР на подгото вку кур.р.	Ина я СР	Контр оль	Все го часо в
	Заняти я лекцио нного типа	Занятия семинарского типа		Контакт ная работа по кур.р.				
		Лаб.р	Прак.					
			/сем.					
Тема 1. Введение в информационную безопасность			2			2		4

Тема 2. Защита от компьютерных вирусов.			10			10		20
Тема 3. Криптографическое закрытие информации			10			10		20
Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств			10			10		20
Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных			10			12		22
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях			8			12		20
Зачет							2	2
Всего часов			50			56	2	108

Таблица 4.3

Содержание разделов дисциплины

Наименование раздела дисциплины	Содержание раздела дисциплины
Тема 1. Введение в информационную безопасность	Роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; проблемы информационной войны; правовые и нормативные акты в области ИБ. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы.

	<p>Особенности программной реализации контроля установленных полномочий. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.</p>
<p>Тема 2. Защита от компьютерных вирусов.</p>	<p>История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановления вычислительной системы после заражения компьютерными вирусами.</p>
<p>Тема 3. Криптографическое закрытие информации</p>	<p>Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.</p>
<p>Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств</p>	<p>Уничтожение остаточных данных. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможностью мгновенного уничтожения данных. Использование общесистемных и специализированных</p>

	<p>программных средств для мгновенного уничтожения данных. Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервирования информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера.</p> <p>Ручное восстановление данных. Безопасное окончание работы на компьютере.</p>
<p>Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных</p>	<p>Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ОС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС (Windows 95, Windows NT, UNIX), их недостатки и основные направления совершенствования. Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод</p>

	обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Типы межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью прокси-серверов. Безопасность JAVA-приложений.

ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

С целью обеспечения эффективного усвоения обучающимися материала курса при выполнении ими лабораторных работ необходимо, чтобы эти работы выполнялись после проработки соответствующего материала и усвоения порядка проведения экспериментальной части. Поэтому допуск обучающихся к выполнению соответствующей работы целесообразно осуществлять только после того, как они во время предварительного опроса покажут соответствующие знания. Таким образом, процедура выполнения обучающимся лабораторной работы сводится к двум этапам: подготовка к собеседованию по теоретической части и выполнение индивидуального практического задания.

Рекомендуется использование компьютеров при выполнении расчетов и исследований в практической работе.

Основная рекомендация сводится к обеспечению равномерной активной работы обучающихся над курсом в течение учебного года: они должны прорабатывать теоретический материал, готовиться к выполнению лабораторных.

Данный курс сориентирован как на самостоятельную познавательную деятельность слушателей, так и на их умение работать с пакетами прикладных программ. При изучении данного курса обучающимся предстоит выполнить следующие виды работ:

- Анализ теоретического материала;
- Проработка лекционного материала;
- Выполнение практических заданий

Тема № 1. Введение в информационную безопасность.

Содержание практического занятия (темы\задания\кейсы\иное)

Задание №1 Управление шаблонами безопасности в Windows

Задание 2 Назначение прав пользователей при произвольном управлении доступом в Windows 2000 (XP)

Основная литература¹

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон.текстовые данные. — Саратов: Профобразование, 2017. — 702 с. -ЭБС «IPRbooks». — 978-5-4488-0070-2. — Режим доступа: <http://www.iprbookshop.ru/63594.html>

Дополнительная литература²

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон.текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. -ЭБС «IPRbooks». — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

Тема № 2. Правовое обеспечение информационной безопасности.

Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 С использованием поисково-справочной системы КонсультантПлюс найти и рассмотреть основные положения нормативных и законодательных актов.

Литература:

Основная

Основная литература³

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон.текстовые данные. — Саратов: Профобразование, 2017. — 702 с. -ЭБС «IPRbooks». — 978-5-4488-0070-2. — Режим доступа: <http://www.iprbookshop.ru/63594.html>

Дополнительная литература⁴

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон.текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. -ЭБС «IPRbooks». — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

Тема № 3. Компьютерные вирусы и борьба с ними.

Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 Профилактика проникновения «троянских программ»

Задание № 2 Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение

Задание № 3 Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение

Основная литература⁵

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон.текстовые данные. — Саратов: Профобразование, 2017. — 702 с.

¹ Из ЭБС института

² Из ЭБС института

³ Из ЭБС института

⁴ Из ЭБС института

⁵ Из ЭБС института

-ЭБС «IPRbooks». — 978-5-4488-0070-2. — Режим доступа:
<http://www.iprbookshop.ru/63594.html>

Дополнительная литература⁶

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон.текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. -ЭБС «IPRbooks». — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

Тема № 4. Восстановление электронной информации. Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 Восстановление зараженных файлов

Задание № 2 Защита программ и файлов от несанкционированного доступа

Основная литература⁷

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон.текстовые данные. — Саратов: Профобразование, 2017. — 702 с. -ЭБС «IPRbooks». — 978-5-4488-0070-2. — Режим доступа:
<http://www.iprbookshop.ru/63594.html>

Дополнительная литература⁸

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон.текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. -ЭБС «IPRbooks». — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

Тема № 5. Электронный документооборот. Электронная цифровая подпись. Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 Установите сертификат удостоверяющего центра и личный служебный сертификат с ключевого носителя.

Основная литература⁹

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон.текстовые данные. — Саратов: Профобразование, 2017. — 702 с. -ЭБС «IPRbooks». — 978-5-4488-0070-2. — Режим доступа:
<http://www.iprbookshop.ru/63594.html>

Дополнительная литература¹⁰

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон.текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. -ЭБС «IPRbooks». — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

⁶ Из ЭБС института

⁷ Из ЭБС института

⁸ Из ЭБС института

⁹ Из ЭБС института

¹⁰ Из ЭБС института

Раздел 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями стандарта ВОв целях реализации компетентного подхода в учебном процессе дисциплины «Основы информационной безопасности в профессиональной деятельности» предусматривается широкое использование активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой. Обсуждение проблем, выносимых на семинарские занятия, лабораторные практикумы и практические занятия, происходит не столько в традиционной форме контроля текущих знаний, сколько в форме дискуссий, сориентированных на творческое осмысление обучающимися наиболее сложных вопросов.

Интерактивные образовательные технологии, используемые на аудиторных практических занятиях

Таблица 5.1

Очная форма обучения

Наименование разделов, тем	Используемые образовательные технологии	Часы
Тема 1. Введение в информационную безопасность	Практикум 1 Круглый стол по вопросам практикума	2
Тема 2. Защита от компьютерных вирусов.	Практикум 2 Круглый стол по вопросам практикума	10
Тема 3. Криптографическое закрытие информации	Практикум 3 Круглый стол по вопросам практикума	10
Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств	Практикум 4 Круглый стол по вопросам практикума	10
Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных	Практикум 5 Круглый стол по вопросам практикума	10
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Практикум 6 Круглый стол по вопросам практикума	10

Практикум

Тема № 1. Введение в информационную безопасность.

Задание №1 Управление шаблонами безопасности в Windows

Краткие теоретические сведения

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации.

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации рассматриваемых операционных систем выполняется в рамках локальной политики безопасности.

Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «Локальная политика безопасности» можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на Вашем компьютере;
- включение и отключение записи действий пользователя или группы в журнале событий.

Задание: настроить параметры локальной политики безопасности операционной системы Windows 2000 (XP).

Алгоритм выполнения работы

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить – Панель управления**.
3. В открывшемся окне выберите ярлык **Администрирование – Локальная политика безопасности** (рис. 25).

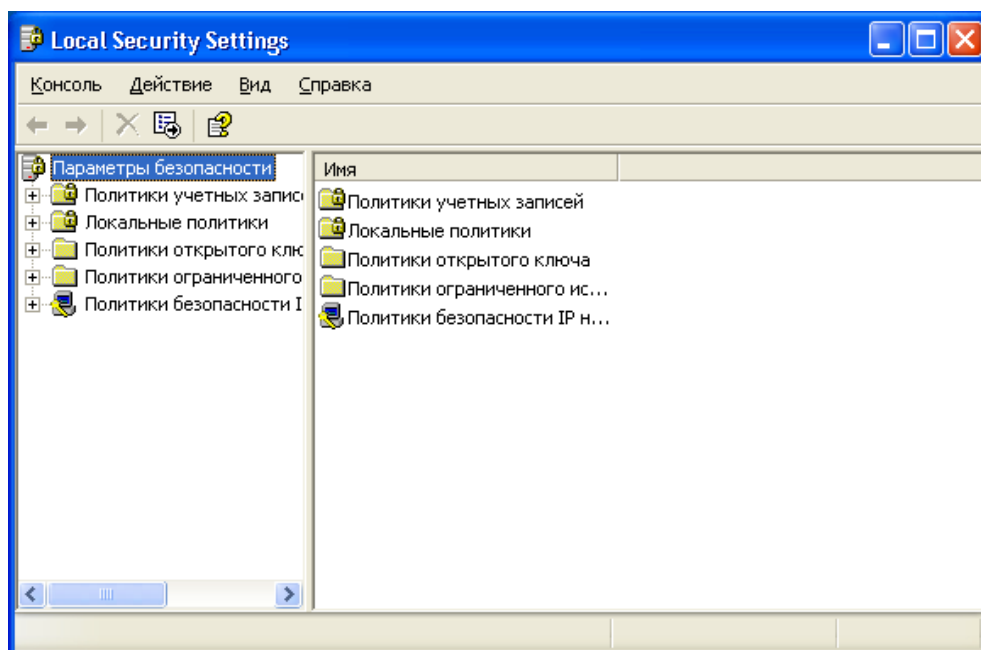


Рис. 25

4. Выберите пункт **Политика учетных записей** (этот пункт включает два подпункта: **Политика паролей** и **Политика блокировки учетной записи**).

5. Откройте подпункт **Политика паролей**. В правом окне появится список настраиваемых параметров (рис. 26).

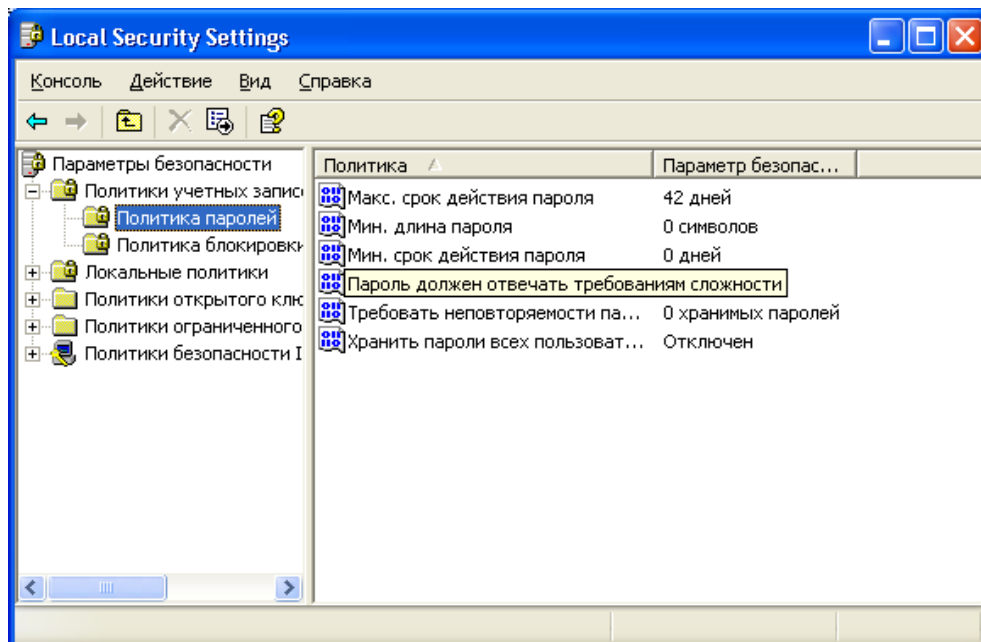


Рис. 26

6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Значения параметров приведены в таблице 6.

7. Ознакомьтесь со свойствами всех параметров.

Таблица 6

Значения параметров Политики паролей

Параметр	Значение
Требовать неповторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24
Максимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней, равным 0
Минимальный срок действия пароля	Определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 999 дней или разрешить немедленное изменение, установив число дней, равным 0
Минимальная длина пароля	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов, равным 0

<p>Пароль должен отвечать требованиям сложности</p>	<p>Определяет, должны ли пароли отвечать требованиям сложности.</p> <p>Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям.</p> <ul style="list-style-type: none"> • Пароль не может содержать имя учетной записи пользователя или какую-либо его часть. • Пароль должен состоять не менее чем из шести символов. • В пароле должны присутствовать символы трех категорий из числа следующих четырех: <ol style="list-style-type: none"> 1) прописные буквы английского алфавита от А до Z; 2) строчные буквы английского алфавита от а до z; 3) десятичные цифры (от 0 до 9); 4) символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %). <p>Проверка соблюдения этих требований выполняется при изменении или создании паролей.</p>
<p>Хранить пароли всех пользователей в домене, используя обратимое шифрование</p>	<p>Определяет, следует ли в системах Windows 2000 Server, Windows 2000 Professional и Windows XP хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, - это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля</p>

8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щелкните на изменяемом параметре).

9. В результате этого действия появится одно из окон, показанных на рисунке 27.

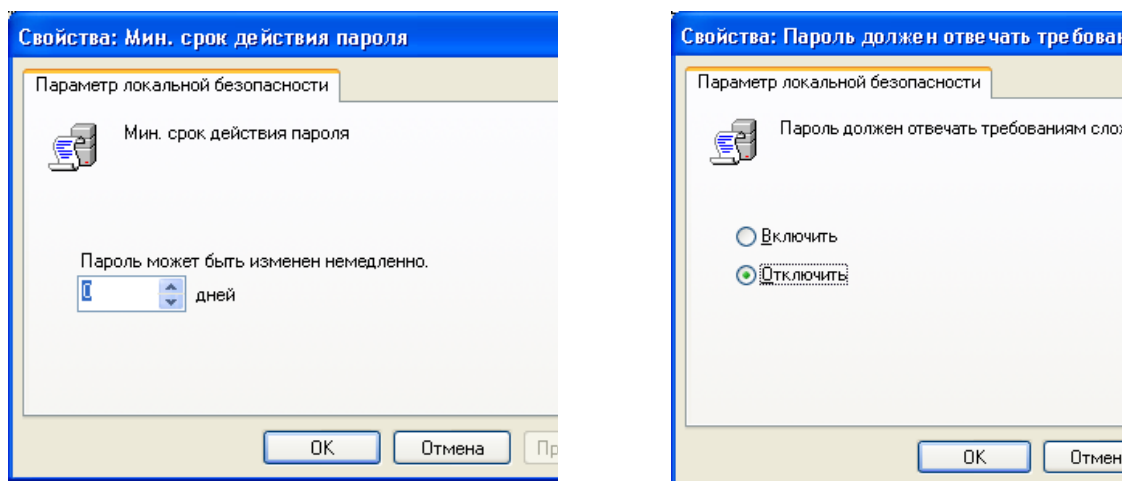


Рис. 27

10. Измените значение параметра и нажмите **Ок**.

11. Например (обязательно выполнить и сохранить), выберите параметр **Требовать неповторяемости паролей** и измените его значение на 1.

12. Для настройки **Политики блокировки учетной записи** выберите этот подпункт и откройте его.

13. Значения параметров данного подпункта Политики учетных записей приведены в таблице 7.
14. Ознакомьтесь со свойствами всех параметров.
15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

Задание 2 Назначение прав пользователей при произвольном управлении доступом в Windows 2000 (XP)

Краткие теоретические сведения

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются **списком ресурсов**, доступным пользователю и **правами доступа** к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Задание: создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и заблокировать учетную запись пользователя.

Алгоритм выполнения работы

А. Создание учетной записи.

1. Откройте оснастку **Управление компьютером** в разделе **Администрирование** **Панели управления** (рис. 31).

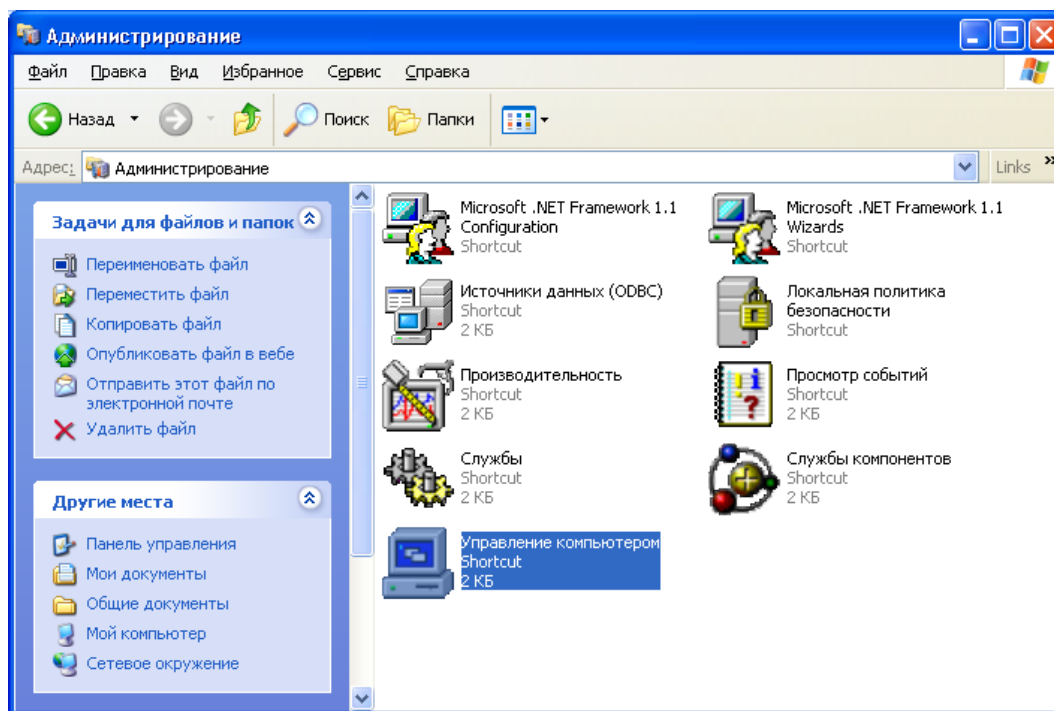


Рис. 31

2. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи** и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Новыйпользователь**(рис. 32). Появится окно диалога**Новыйпользователь**(рис. 33).

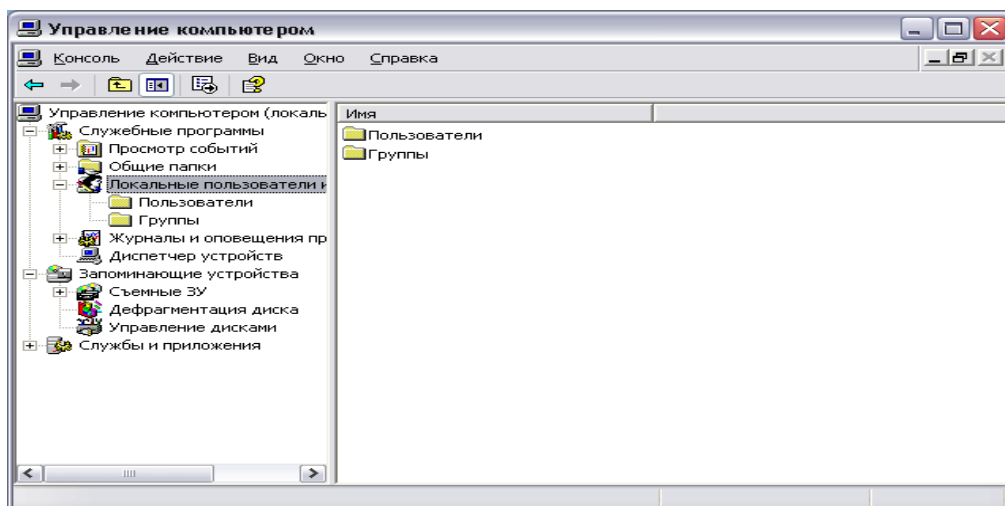


Рис. 32

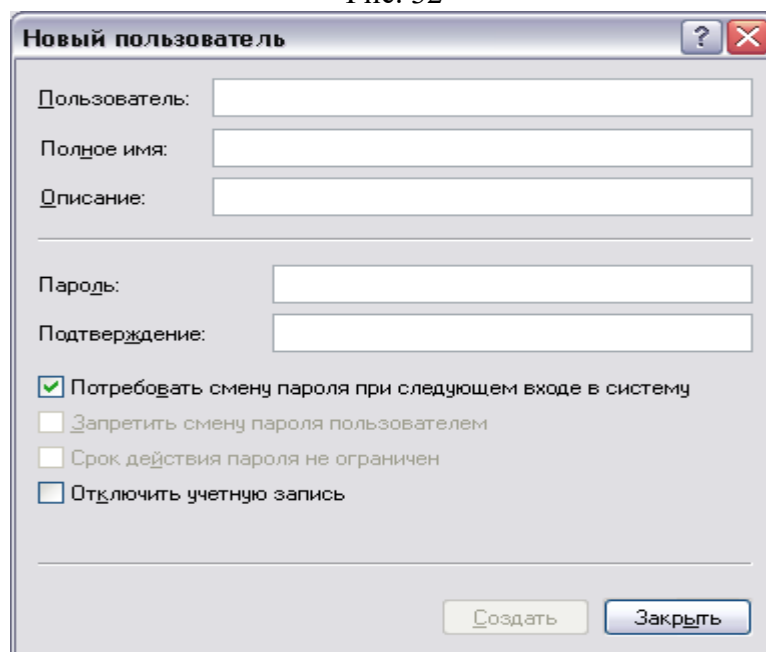


Рис.33

4. В поле **Пользователь** введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо: » / \ [] : ; = , +*?<>Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле **Полное имя** введите полное имя создаваемого пользователя.

6. В поле **Описание** введите описание создаваемого пользователя или его учетной записи, например, «студент.....».

7. В поле **Пароль** введите пароль пользователя и в поле **Подтверждение** подтвердите его правильность вторичным вводом.

Примечание: длина пароля не может превышать 14 символов.

8. Установите или снимите флажки:

- потребовать смену пароля при следующем входе в систему;
- запретить смену пароля пользователем;
- срок действия пароля не ограничен;

- отключить учетную запись.

9. Чтобы создать еще одного пользователя, нажмите кнопку **Создать** и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку **Создать** и затем **Заккрыть**.

В. Создание локальной группы.

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Новая группа**.

3. В поле **Имя группы** (рис. 34) введите имя новой группы, например, **Студенты**.

Примечание: имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле **Описание** введите описание новой группы.

5. В поле **Члены группы** можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку **Добавить** и выбрать их в списке.

Для завершения нажмите кнопку **Создать** и затем **Заккрыть**.

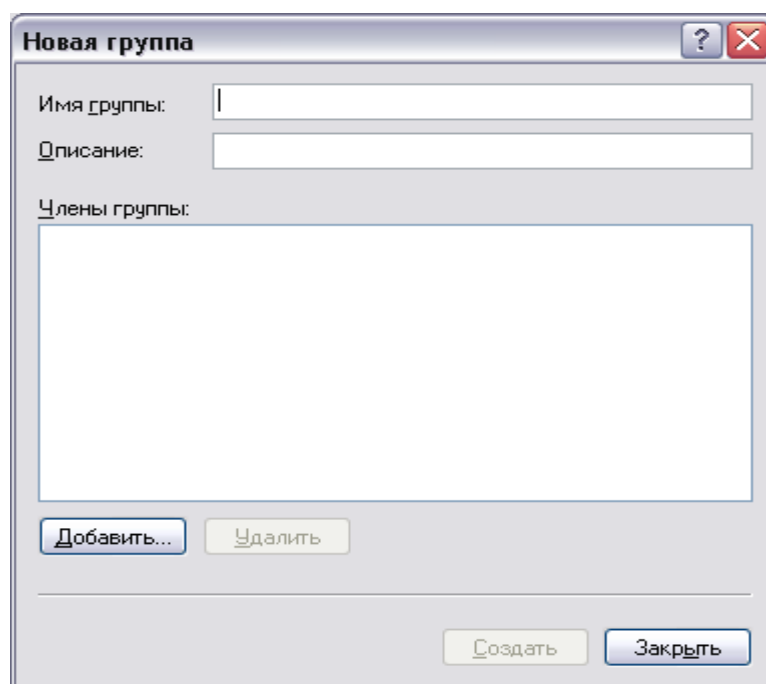


Рис.34

С. Изменение членства в локальной группе.

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы**.

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Добавить в группу** или **Свойства**.

4. Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить** (рис. 35).

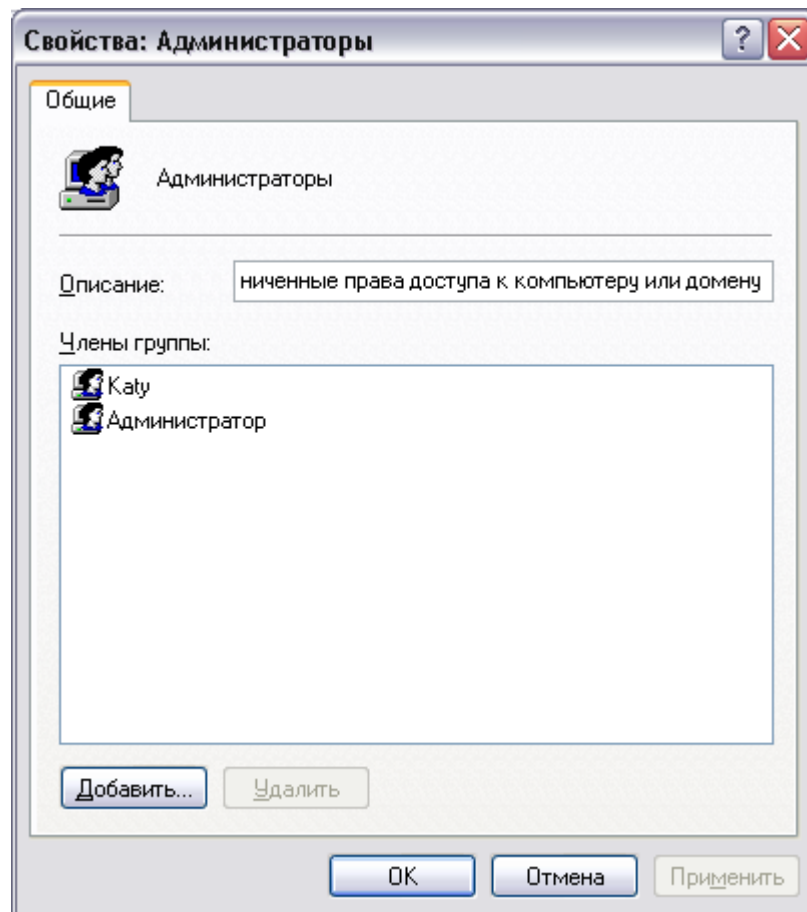


Рис.35

5. Далее следуйте указаниям окна диалога **Выбор: Пользователи или Группы**.

6. Для того, чтобы удалить из группы некоторых пользователей, в поле **Члены группы** (рис. 35) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить**.

Примечание. В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

D. Временная блокировка учетной записи.

1. Откройте оснастку **Управление компьютером**.

2. Для этого либо выберите на Рабочем столе ярлык **Мой компьютер** и нажмите правую клавишу мыши, после чего выберите пункт контекстного меню **Управление**, либо воспользуйтесь разделом **Администрирование** в Панели управления.

3. В открывшейся оснастке выберите пункты **Службные программы/Локальные пользователи и группы** (рис. 32).

4. Откройте папку **Пользователи** и выберите учетную запись **Гость**.

5. Нажмите правую клавишу мыши и выберите пункт **Свойства**.

6. В открывшемся окне снимите отметку пункта **Отключить учетную запись** (рис. 36).

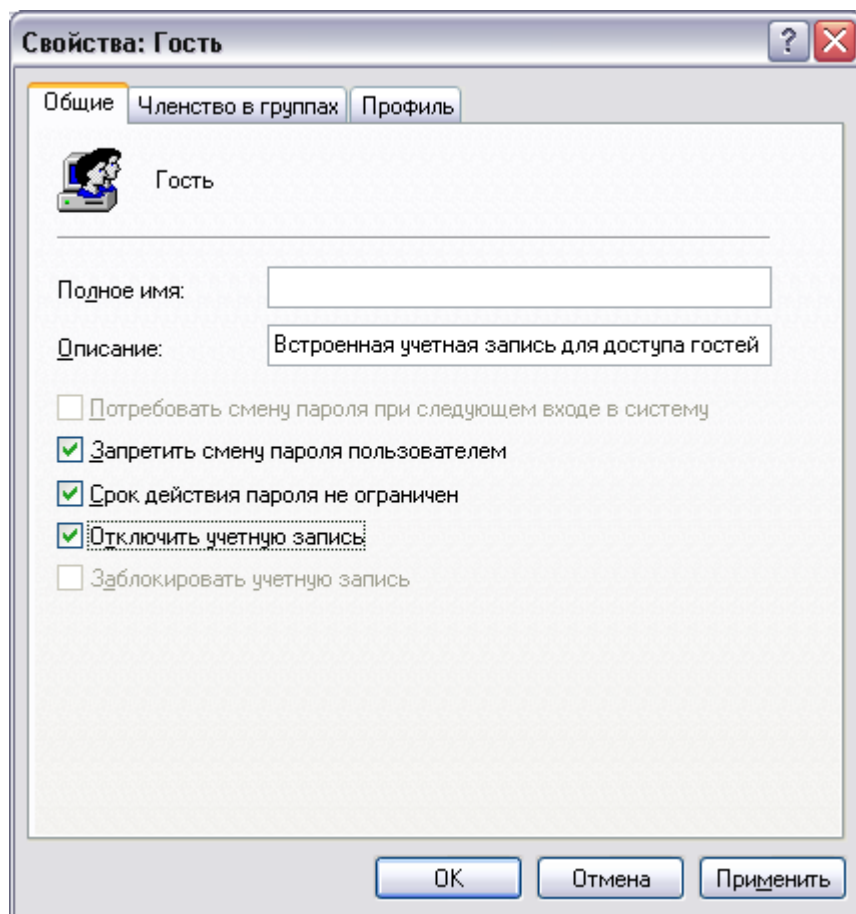


Рис. 36

7. Нажмите кнопку **OK** и сделайте вывод о состоянии учетной записи.
8. Выполните пункт 5 и отметьте пункт **Отключить учетную запись**.

Тема № 2. Правовое обеспечение информационной безопасности.

Законодательные аспекты защиты информации

Задание № 1 С использованием поисково-справочной системы КонсультантПлюс найти и рассмотреть основные положения нормативных и законодательных актов:

«О государственной тайне» (№ 5485-1 от 21.07.1993 г.);

«Об участии в международном информационном обмене» (№ 85ФЗ от 5.06.1996 г.);

«Об электронной цифровой подписи» (№ 1-ФЗ от 10.01.2002 г.);

«О коммерческой тайне» (№ 98-ФЗ от 29.07.2004 г.);

«Об информации, информационных технологиях и о защите информации» (от 27.08.2006 г. № 149 - ФЗ);

«О персональных данных» (№ 152-ФЗ от 27.07.2006 г.).

Постановление Правительства РФ от 17.11. 2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (ПП РФ № 781 от 17.11. 2007г.);

Постановление Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (ПП РФ № 687 от 15.09.2008);

Нормативно-методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден Приказом заместителя директора ФСТЭК 15.02.2008;

Нормативно-методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден Приказом заместителя директора ФСТЭК 15.02.2008.

Предмет и объект защиты информации

Задание. 2 С использованием поисково-справочной системы КонсультантПлюс найти и рассмотреть основные положения следующих нормативных и законодательных актов:

Нормативно-методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден Приказом заместителя директора ФСТЭК 15.02.2008;

Нормативно-методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден Приказом заместителя директора ФСТЭК 15.02.2008.

Введение

Каждый человек в своей жизни сталкивается с необходимостью поиска и анализа правовой информации в рамках его профессиональной деятельности или в различных житейских ситуациях (чтобы выяснить свои права как гражданина, защитить свои права как потребителя, оформить сделки и пр.). Надежным и эффективным помощником в таких случаях является СПС КонсультантПлюс — система, направленная на легкий, удобный, быстрый поиск и анализ правовой информации.

Самая полная база правовой информации более 150 млн. документов.

Уникальные аналитические материалы описывают порядок решения большинства практических вопросов, которые возникают в работе специалистов, на основе законодательства и сложившейся судебной практики

Простой и быстрый поиск информации.

Поисковые инструменты в системе КонсультантПлюс разработаны специально для работы с правовой информацией, при этом они учитывают профессиональную лексику и распространенные сокращения.

Важная информация о применении нормативных актов включена в тексты.

В КонсультантПлюс все нормативные акты снабжены важной информацией об их применении — ясно, действует документ или нет; в тексте есть примечания об особенностях, которые нужно учитывать; к каждой статье подобраны консультации, разъяснения и судебная практика.

Онлайн-сервисы

«Конструктор договоров» и «Конструктор учетной политики» особые инструменты в системе КонсультантПлюс, они позволяют составлять и анализировать договоры и учетную политику компании на принципиально новом уровне.

Персональные профили для каждого специалиста

Для бухгалтера, юриста, специалиста бюджетной организации, специалиста по закупкам, специалиста по кадрам. Свой профиль — это стартовая страница, лента новостей, специальные подсказки и результаты поиска, настроенные под задачи специалиста.

Система КонсультантПлюс в отличие от многих иных источников правовой информации (в том числе в интернете) позволяет решать вопросы доступа к правовой информации комплексно: не просто найти документы по интере-

сущему вас вопросу, но и получить разъяснения, узнать порядок действий по ситуации, выявить спорные моменты, а также в удобном виде сохранить результаты работы с найденными документами.

Очень важно также, что вы можете быть уверенными в актуальности представленной информации.

Какие материалы есть в системе КонсультантПлюс?

Для удобства поиска информации все документы содержатся в **Едином информационном массиве** КонсультантПлюс.

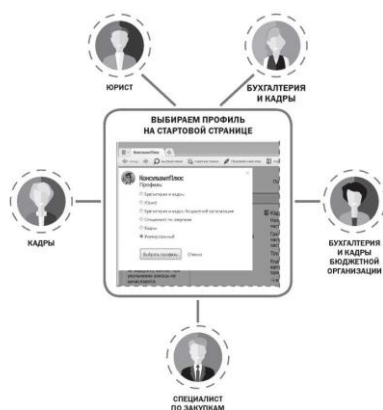
Единый информационный массив разбит на **10 разделов**, объединяющих документы определенного типа (например, нормативные акты, материалы судебной практики, финансовые консультации и т.д.). Каждый из разделов содержит один или несколько близких по содержанию **информационных банков (ИБ)**, например, раздел с нормативными актами содержит информационный банк с нормативными актами федерального уровня и информационные банки с нормативными актами отдельных субъектов РФ.

С чего начать работу в системе?

Для запуска системы используется ярлык КонсультантПлюс на рабочем столе.

После запуска откроется стартовая страница КонсультантПлюс, откуда можно перейти к различным поисковым инструментам системы, в зависимости от характера имеющихся у вас сведений.

Чтобы обеспечить специалисту максимально быстрый доступ к нужной информации, систему КонсультантПлюс можно настроить под его профессиональные задачи, выбрав соответствующий профиль. Для этого достаточно нажать на кнопку рядом с текущим профилем (возле логотипа КонсультантПлюс в левом верхнем углу (рис. 1)).



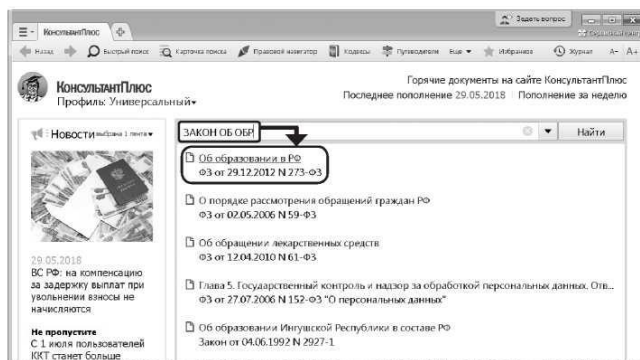


Рис. 1. Выбор профиля на стартовой странице

Специализированный профиль — это своя стартовая страница, лента новостей, специальные подсказки и результаты поиска, подстроенные под задачи специалиста (рис. 2). Доступен также профиль «Универсальный».



Рис. 2. Стартовая страница профиля «Бухгалтерия и кадры»



Как искать информацию в системе КонсультантПлюс

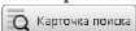
Поиск документа или его фрагмента

Наиболее простой способ поиска документов в системе — Быстрый поиск. Он доступен со стартовой страницы, а также из любого другого места системы через панель инструментов или при выборе вкладки И сразу готов к работе.



1.3. Поиск документа по реквизитам


 Видеоролик «Карточка поиска и ее специальные возможности» смотрите на сайте <http://www.consultant.ru/edu/> в разделе «Обучение КонсультантПлюс онлайн».
 

В системе КонсультантПлюс кроме Быстрого поиска есть и другие инструменты поиска документов, в частности, Карточка поиска (рис. 1.4). Перейти в нее можно по ссылке со стартовой страницы, а также из любого другого места системы с помощью кнопки  панели инструментов.

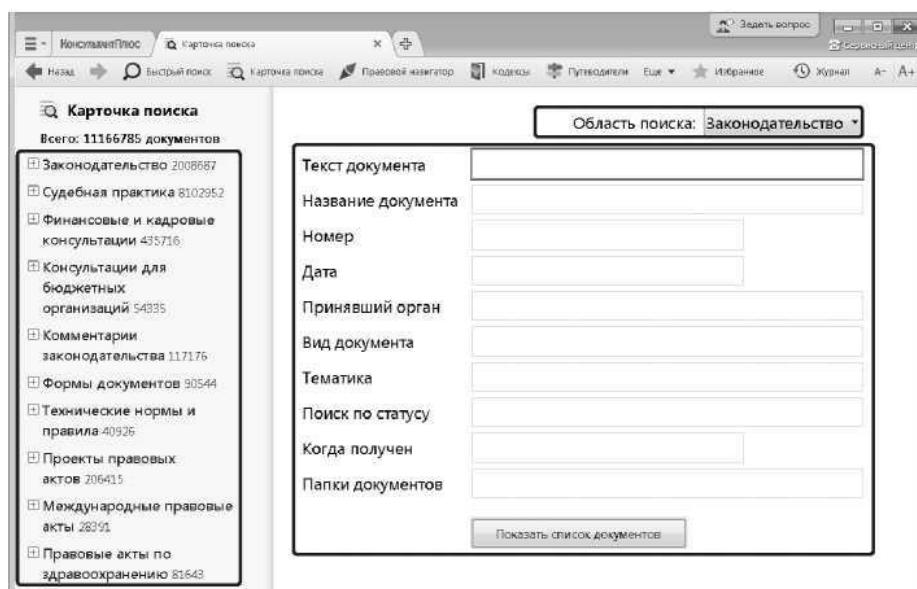
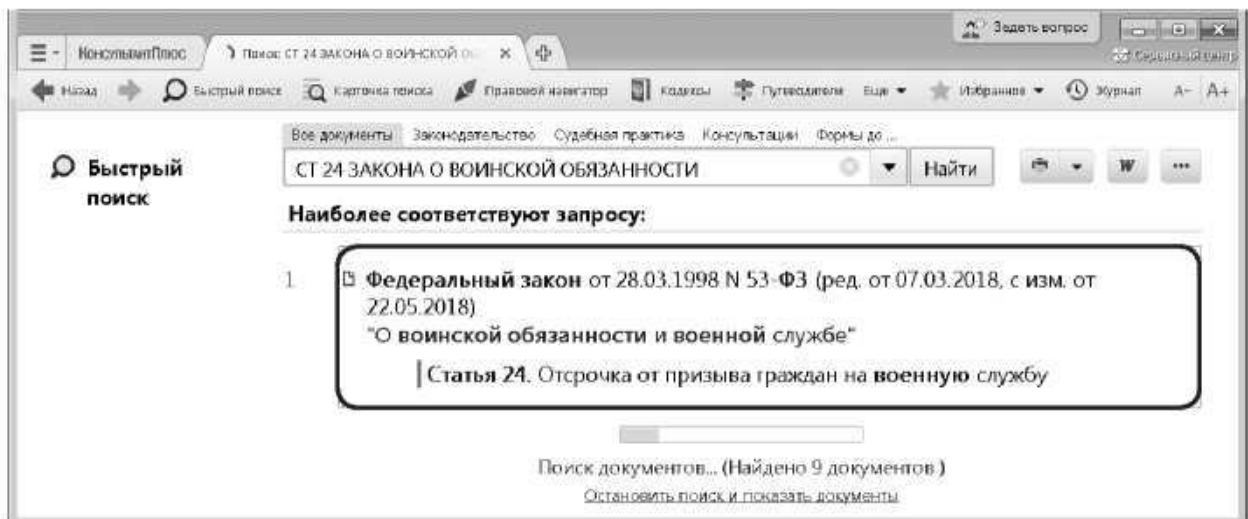


Рис. 1.4. Карточка поиска КонсультантПлюс

Рис.3. Поиск документа или его фрагмента

1.1. Быстрый поиск документа

При поиске конкретного документа можно задать два-три важных слова из его названия, вид документа, а также указать другие реквизиты. В запросе можно использовать общепринятые сокращения и аббревиатуры.



Пример 1.2. Найдем ст. 24 Федерального закона «О воинской обязанности и военной службе», касающуюся предоставления отсрочки от призыва.

1. Зададим в строке Быстрого поиска: СТ 24 ЗАКОНА О ВОИНСКОЙ ОБЯЗАННОСТИ.
2. Нажмем кнопку .
3. Наиболее соответствующие запросу документы появляются сразу, до построения всего списка (рис. 1.3).
4. Щелкнем по ссылке на нужную статью под названием закона (рис. 1.3). Документ сразу откроется на ст. 24.

Результаты Быстрого поиска появляются поэтапно. По запросам с подсказкой первые несколько документов отображаются практически одновременно с нажатием на кнопку (рис. 1.3), а пока пользователь их просматривает, список документов достраивается полностью.

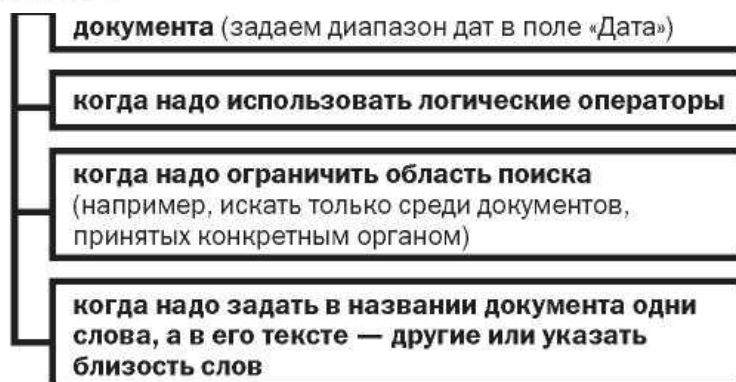


Рис. 1.5. Возможности Карточки поиска

В поле «Текст документа» рекомендуется указывать слова или фразы, которые наверняка есть в тексте документа. Слова нужно задавать полностью, можно использовать общепринятые сокращения и аббревиатуры. Следует избегать длинных фраз: в этом случае увеличивается вероятность того, что одно из слов такой фразы может отсутствовать в тексте документа.

Во вкладке «Задать» поля «Дата» можно воспользоваться встроенным календарем (рис. 1.6).

Карточкой поиска удобно пользоваться, если надо задать логические условия.

ПРИМЕР 1.4. Найдем документ, которым направлено разъяснение о том, облагается ли повышенная стипендия налогом. При этом мы точно не знаем, кем принят этот документ: то ли Минобразованием РФ, то ли Рособразованием, то ли Минобрнауки РФ.

1. Откроем Карточку поиска.
2. В поле «Принявший орган» последовательно выберем значения: *МИНОБРНАУКИРФ*, *РОСОБРАЗОВАНИЕ*, *МИНОБРАЗОВАНИЕРФ*, отмечая их каждый раз галочкой (рис. 1.7).
3. Соединим их логическим условием или (рис. 1.7).
4. В поле «Текст документа» введем: стипендия налог.
5. Нажмем КНОПКУ [Показать список документов].
6. Будет найдено Письмо Рособразования от 15.03.2005 № 16-55-69ин/04-06<Об освобождении от налогообложения стипендий>, из которого мы узнаем, что студенческие стипендии НДФЛ не облагаются.



Рис. 1.8. Как работает Быстрый поиск

Рис. 1.7. Выбор логического условия в словаре поля Карточки поиска

В поле «Принявший орган» (а также в других полях) можно выбирать несколько значений и соединять их различными логическими условиями (рис. 1.7): логическим условием *И*, чтобы найти документ, принятый совместно несколькими органами, логическим условием *ИЛИ*, если вы затрудняетесь точно определить, какой именно орган принял искомый

документ (как в приведенном выше примере), логическим условием *КРОМЕ*, если надо исключить какие-то значения из поиска.

Поиск ответа на практический вопрос

Рассмотрим вопросы поиска правовой информации по практическому вопросу, если заранее неизвестно, в каких документах она может содержаться.

Наиболее удобный инструмент поиска в такой ситуации — Быстрый поиск, работать с ним просто (рис. 1.8).

ПРИМЕР 1.5. *Выясним, какова продолжительность отпуска для сдачи госэкзаменов работникам-студентам, обучающимся по заочной форме обучения.*

1. В строке Быстрого поиска зададим: `ОТПУСК ДЛЯ СДАЧИ ГОСЭКЗАМЕНОВ И` и нажмем кнопку .
2. В начале списка найденных документов содержится Трудовой кодекс РФ. Откроем его.
3. Документ откроется на фрагменте ст. 173, в котором указано, что продолжительность отпуска для прохождения государственной итоговой аттестации — до четырех месяцев в соответствии с учебным планом осваиваемой работником образовательной программы высшего образования.

Результатом Быстрого поиска является список документов, наиболее соответствующих поисковому запросу (не более 50 документов). Будут найдены правовые акты, консультации, судебные решения и другие материалы.

В начале списка находятся документы, наиболее точно отвечающие запросу в соответствии с выбранным профилем (для бухгалтера выше размещаются бухгалтерские документы).

Для удобства работы со списком содержательная часть названия выделяется.

ПРИМЕР 1.6. *Выясним, как поехать учиться за границу по обмену.*

1. В строке Быстрого поиска зададим: `УЧИТЬСЯ ПО ОБМЕНУ` и нажмем кнопку .
2. Откроем материал «Ситуация: Как поехать учиться по обмену?» из электронного журнала «Азбука права».
3. В консультации подробно рассмотрено, какие шаги следует предпринять для того, чтобы поехать учиться по обмену, какие документы следует подготовить, представлена ссылка на соответствующую статью закона об образовании. Указано, куда можно обратиться, если ни один из предложенных вашим вузом вариантов не устраивает. Отмечены возможные риски.

В системе КонсультантПлюс есть консультации из электронного журнала «Азбука права» с короткими понятными ответами на повседневные правовые вопросы личного характера (см. пример 1.6). Консультации даны в виде пошаговых инструкций и касаются таких актуальных тем, как автомобиль, воинская обязанность, выезд за границу, образование, семья, труд и др.

Материалы «Азбуки права» включены в информационный банк «Бухгалтерская пресса и книги» (раздел «Финансовые и кадровые консультации»).

По запросу в Быстром поиске можно построить полный список документов из всех разделов и информационных банков, например, когда нужны все консультации или вся судебная практика для детального изучения проблемы. Для этого воспользуйтесь ссылкой «Все результаты поиска» под строкой Быстрого поиска.

Тема № 3. Компьютерные вирусы и борьба с ними.

Задание № 1 Проверка и защита компьютера от вирусов

1. Создайте в рабочей папке тестовый вирус EICAR1 (Тестовый вирус был специально разработан организацией EICAR (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов. Тестовый вирус не является вредоносной программой (не содержит программного кода, который может навредить вашему компьютеру), при этом большинство антивирусов идентифицируют его как вирус) с помощью текстового редактора Блокнот - файл eicar.com и наберите в нем текст: X5O!P% @AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Если на компьютере установлена фоновая (резидентная) проверка файлов, то Вы не сможете сохранить данный файл, он будет автоматически удаляться антивирусной программой.

2. Откройте антивирусную программу, изучите установленные параметры ее работы и получите справку по их содержанию и настройке.

3. Настройте программу на проверку загрузочного сектора, всех файлов, файлов в архивах и упакованных. Установите действие при обнаружении вируса - Лечить и включите опцию Запрос подтверждения.

4. Протестируйте рабочую папку. В случае обнаружения вирусов выберите опцию Лечить, а если это невозможно, то Удалить.

5. Изучите отчет о тестирования.

6. Закройте антивирусную программу.

Задание № 2 Профилактика проникновения «троянских программ»

Краткие теоретические сведения

Главное отличие «троянских программ» от компьютерных вирусов состоит в том, что они не размножаются на зараженном компьютере и не имеют встроенных возможностей к самораспространению. «Троянские кони» засылаются пользователям (обычно через электронную почту) непосредственно их авторами под видом каких-нибудь полезных утилит. На самом деле они производят несанкционированное внедрение на компьютеры и в

корпоративные сети различного рода нежелательных программ. Именно этой особенности «Троянские кони» обязаны своим названием.

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере.

Backdoor – троянские утилиты удаленного администрирования

Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске «троянец» устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на «троянца» может отсутствовать в списке активных приложений. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Утилиты скрытого управления позволяют делать с компьютером все, что в них заложил автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти троянцы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п. – пораженные компьютеры оказываются открытыми для злоумышленных действий хакеров.

Таким образом, троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, присущих другим видам троянских программ.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают компьютерные черви. Отличает такие «троянцы» от червей тот факт, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

Trojan-PSW – воровство паролей

Данное семейство объединяет троянские программы, «ворующие» различную информацию с зараженного компьютера, обычно – системные пароли (PSW – Password-Stealing-Ware). При запуске PSW-троянцы ищут системные файлы, хранящие различную конфиденциальную информацию (обычно номера телефонов и пароли доступа к интернету) и отсылают ее по указанному в коде «троянца» электронному адресу или адресам.

Существуют PSW-троянцы, которые сообщают и другую информацию о зараженном компьютере, например, информацию о системе (размер памяти и дискового пространства, версия операционной системы), тип используемого почтового клиента, IP-адрес и т.п. Некоторые троянцы данного типа «воруют» регистрационную информацию к различному программному обеспечению, коды доступа к сетевым играм и прочее.

Trojan-AOL – семейство троянских программ, «ворующих» коды доступа к сети AOL (AmericaOnline). Выделены в особую группу по причине своей многочисленности.

Trojan-Clicker – интернет-кликеры

Семейство троянских программ, основная функция которых – организация несанкционированных обращений к интернет-ресурсам (обычно к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса интернет-ресурсов (например, файл hosts в MS Windows).

У злоумышленника могут быть следующие цели для подобных действий:
увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;
организация DoS-атаки (DenialofService) на какой-либо сервер;
привлечение потенциальных жертв для заражения вирусами или троянскими программами.

Trojan-Downloader – доставка прочих вредоносных программ

Троянские программы этого класса предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки «троянцев» или рекламных систем. Загруженные из интернета программы затем либо запускаются на выполнение, либо регистрируются «троянцем» на автозагрузку в соответствии с возможностями операционной системы. Данные действия при этом происходят без ведома пользователя.

Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с «управляющего» интернет-ресурса (обычно с веб-страницы).

Trojan-Dropper – инсталляторы прочих вредоносных программ

Троянские программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ.

Данные троянцы обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве или неверной версии операционной системы) сбрасывают на диск в какой-либо каталог (в корень диска C:, во временный каталог, в каталоги Windows) другие файлы и запускают их на выполнение.

Обычно структура таких программ следующая:

Основной код
Файл 1
Файл 2
...

«Основной код» выделяет из своего файла остальные компоненты (файл 1, файл 2, ...), записывает их на диск и открывает их (запускает на выполнение).

Обычно один (или более) компонент является троянской программой, и как минимум один компонент является «обманкой»: программой-шуткой, игрой, картинкой или чем-то подобным. «Обманка» должна отвлечь внимание пользователя и/или продемонстрировать то, что запускаемый файл действительно делает что-то «полезное», в то время как троянская компонента инсталлируется в систему.

В результате использования программ данного класса хакеры достигают двух целей:

- скрытная инсталляция троянских программ и/или вирусов;
- защита от антивирусных программ, поскольку не все из них в состоянии проверить все компоненты внутри файлов этого типа.

Trojan-Proxy – троянские прокси-сервера

Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным интернет-ресурсам. Обычно используются для рассылки спама.

Trojan-Spy – шпионские программы

Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайн-платежей и банковских систем.

Trojan – прочие троянские программы

К данным троянцам относятся те из них, которые осуществляют прочие действия, попадающие под определение троянских программ, т.е. разрушение или злонамеренная модификация данных, нарушение работоспособности компьютера и прочее.

В данной категории также присутствуют «многоцелевые» троянские программы, например, те из них, которые одновременно шпионят за пользователем и предоставляют ргоху-сервис удаленному злоумышленнику.

Trojan-Notifier – оповещение об успешной атаке

Троянцы данного типа предназначены для сообщения своему «хозяину» о зараженном компьютере. При этом на адрес «хозяина» отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т.п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице «хозяина», ICQ-сообщением.

Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего «хозяина» об успешной инсталляции троянских компонент в атакуемую систему.

Реестр операционной системы Windows – это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. Реестр содержит данные, к которым Windows XP постоянно обращается во время загрузки, работы и её завершения, а именно:

- профили всех пользователей, то есть их настройки;
- конфигурация оборудования, установленного в операционной системе.
- данные об установленных программах и типах документов, создаваемых каждой программой;
 - свойства папок и значков программ;
 - данные об используемых портах.

Реестр имеет иерархическую древовидную структуру, состоящую из разделов, подразделов и ключей (параметров).

В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь

копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «Редактор реестра».

Файл редактора реестра находится в папке Windows. Называется он regedit.exe. Для того, чтобы запустить эту программу, необходимо выбрать Пуск – Выполнить – regedit.exe. После запуска появится окно редактора реестра. Вы увидите список из 5 разделов (рис. 11):

HKEY_CLASSES_ROOT.
HKEY_CURRENT_USER.
HKEY_LOCAL_MACHINE.
HKEY_USERS.
HKEY_CURRENT_CONFIG.

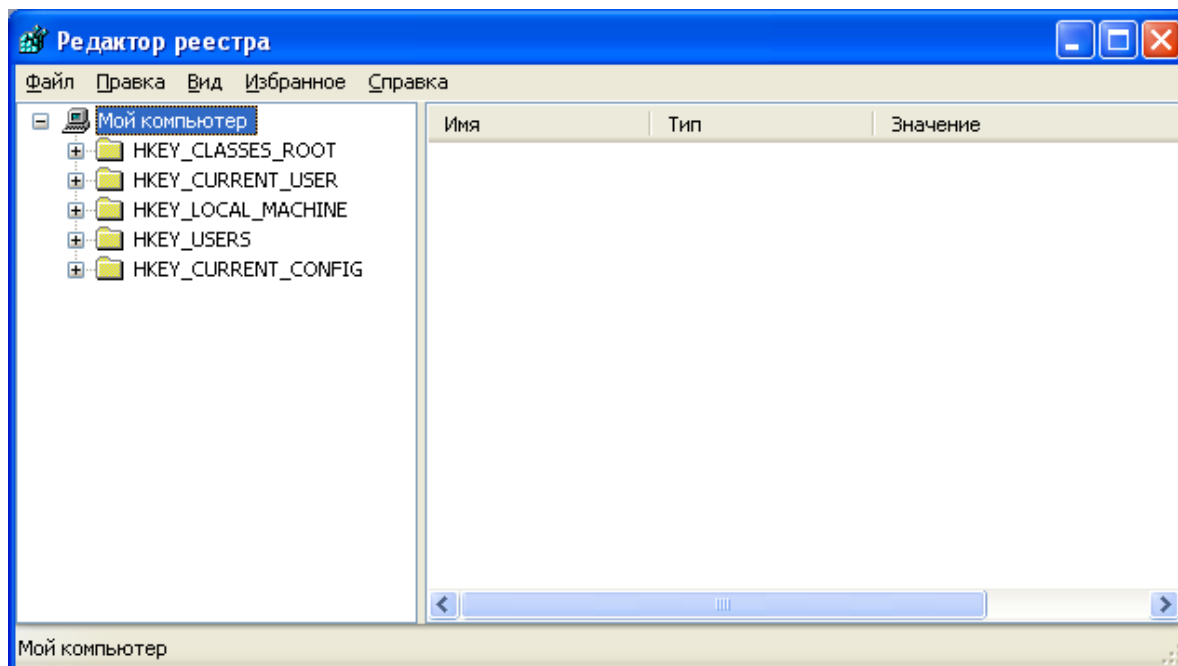


Рис. 11

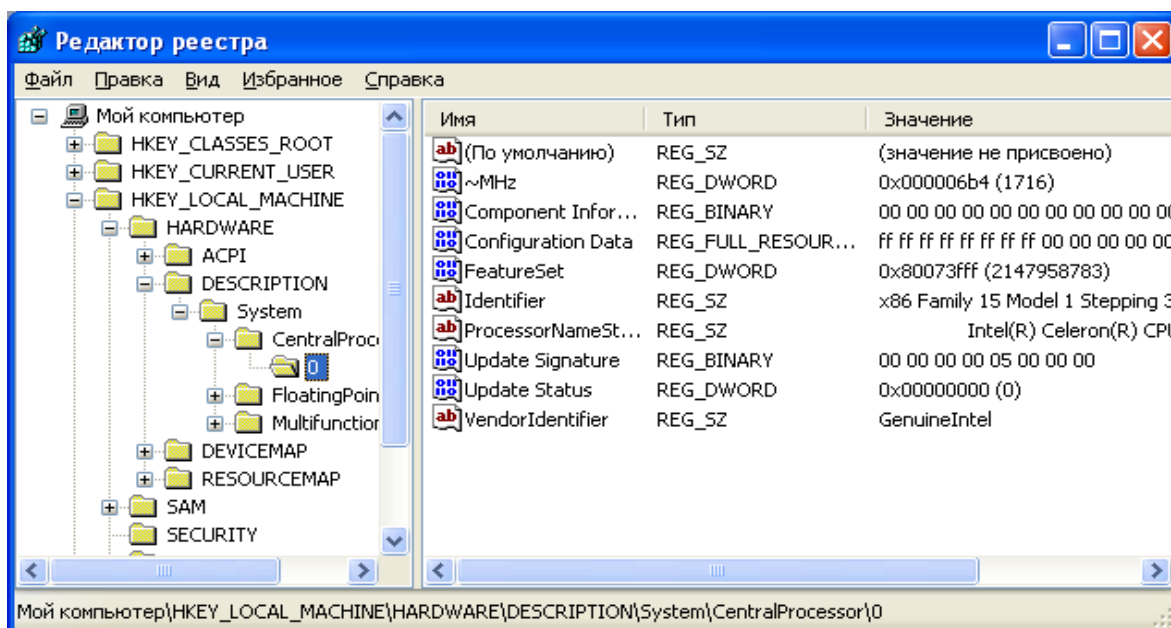


Рис. 12

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа (рис. 12):

- строковые (напр. «C:\Windows»);

- двоичные (напр. 10 82 AO 8F);

DWORD - этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

В Windows системная информация разбита на так называемые ульи (hive). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist** (рис. 13).

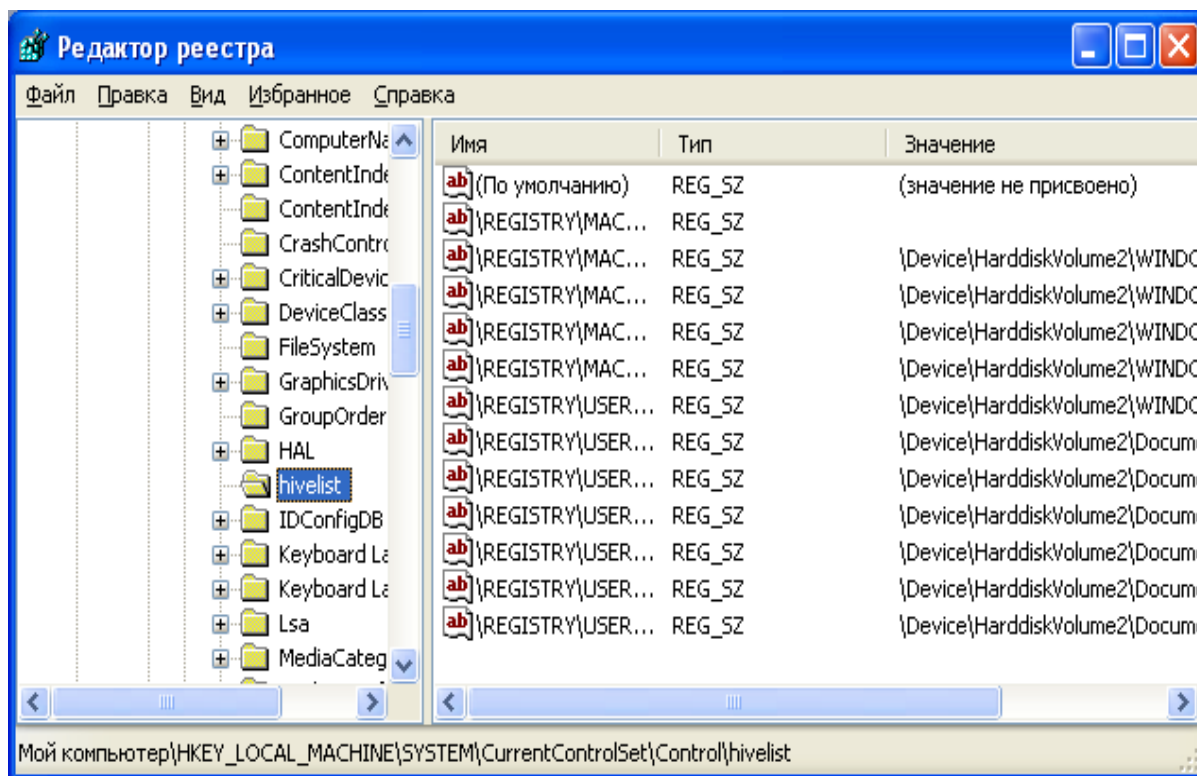


Рис. 13

В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 5

Характеристика основных разделов системного реестра

HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (SecurityAccessManager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке %Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SECURITY	Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config
HKEY_USERS\DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового

	пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Config
HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\Username, где Username – имя пользователя

Задание: проверить потенциальные места записей «троянских программ» в системном реестре операционной системы Windows 2000 (XP).

Алгоритм выполнения работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу **regedit.exe**.
2. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\ Microsoft\ WindowsNT\ CurrentVersion\ Winlogon** (щелкнуть по значку «папка»).
3. В правой половине открытого окна программы **regedit.exe** появится список ключей.
4. Найдите ключ **Userinit (REG_SZ)** и проверьте его содержимое.
5. По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись **C:\WINDOWS\system32\userinit.exe** (рис. 14).

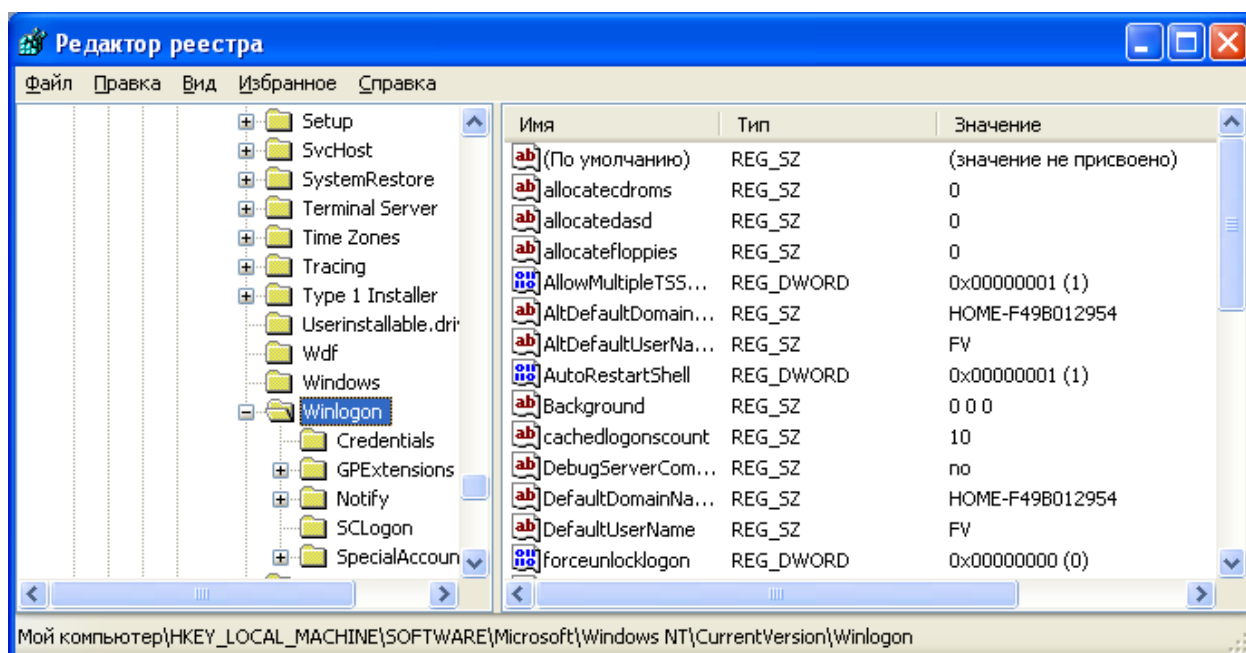


Рис. 14

6. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».
7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.
8. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».
9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы **regedit.exe**).

10. В открывшемся окне в поле **Значение** (рис. 15) удалите ссылку на подозрительный файл.

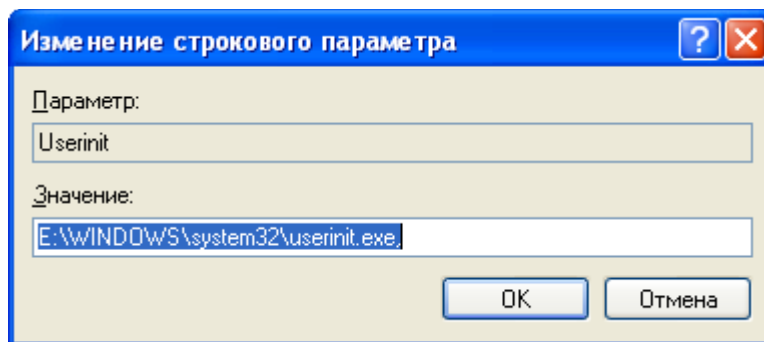


Рис. 15

11. Закройте программу **regedit.exe**.
12. Перейдите в папку с подозрительным файлом и удалите его.
13. Перезагрузите операционную систему и выполните пункты задания 1-4.
14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска **Run**.

Для его проверки выполните следующее.

1. Запустите программу **regedit.exe**.
2. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\Microsoft\Windows\CurrentVersion\Run\...** (**REG_SZ**) (рис. 16).

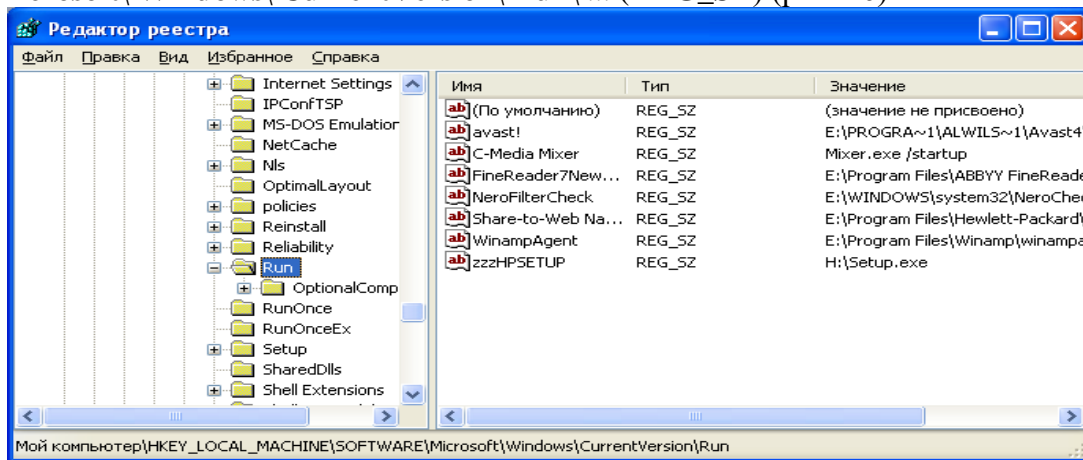


Рис. 16

3. В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).

4. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

Задание № 3 Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение

Общие сведения

Пользователи ПК наиболее часто сталкиваются с одной из разновидностей

компьютерной преступности □ компьютерными вирусами. Последние являются особого типа вредоносными программами, доставляющими пользователям и обслуживающему ПК персоналу немало неприятностей.

Компьютерным вирусом называется способная к самовоспроизводству и размножению программа, внедряющаяся в другие программы.

Очевидна аналогия понятий компьютерного и биологического вирусов. Однако не всякая могущая саморазмножаться программа является компьютерным вирусом. Вирусы всегда наносят ущерб □ препятствуют нормальной работе ПК, разрушают файловую структуру и т.д., поэтому их относят к разряду так называемых вредоносных программ.

Исторически появление компьютерных вирусов связано с идеей создания самовоспроизводящихся механизмов, в частности программ, которая возникла в 50-х гг. Дж.фон Нейман еще в 1951 г. предложил метод создания таких механизмов, и его соображения получили дальнейшее развитие в работах других исследователей. Первыми появились игровые программы, использующие элементы будущей вирусной технологии, а затем уже на базе накопленных научных и практических результатов некоторые лица стали разрабатывать самовоспроизводящиеся программы с целью нанесения ущерба пользователям компьютера.

Основными каналами проникновения вирусов в персональный компьютер являются накопители на сменных носителях информации и средства сетевой коммуникации, в частности сеть Internet.

В настоящее время в мире насчитывается более 20 тысяч вирусов, включая штаммы, т.е. разновидности вирусов одного типа. Вирусы не признают границ, поэтому большинство из них курсирует и по России. Более того, проявилась тенденция увеличения числа вирусов, разработанных отечественными программистами. Если ситуация не изменится, то в будущем Россия сможет претендовать на роль лидера в области создания вирусов.

Классификация вирусов

Жизненный цикл компьютерных вирусов, как правило, включает следующие фазы:

- латентный период, в течение которого вирусом никаких действий не предпринимается;
- инкубационный период, в пределах которого вирус только размножается;
- активный период, в течение которого наряду с размножением выполняются несанкционированные действия, заложенные в алгоритме вируса.

Первые две фазы служат для того, чтобы скрыть источник вируса, канал его проникновения и инфицировать как можно больше файлов до выявления вируса. Длительность этих фаз может определяться предусмотренным в алгоритме временным интервалом, наступлением какого-либо события в системе, наличием определенной конфигурации аппаратных средств ПК (в частности, наличием НЖМД) и т.д.

Компьютерные вирусы классифицируются в соответствии со следующими признаками:

- среда обитания;
- способ заражения среды обитания;
- способ активизации;
- способ проявления (деструктивные действия или вызываемые эффекты);
- способ маскировки.

Вирусы могут внедряться только в программы, которые, в свою очередь, могут содержаться или в файлах, или в некоторых компонентах системной области диска, участвующих в процессе загрузки операционной системы. В соответствии со средой обитания различают:

- файловые вирусы, инфицирующие исполняемые файлы;
- загрузочные вирусы, заражающие компоненты системной области, используемые при загрузке ОС;
- файлово-загрузочные вирусы, интегрирующие черты первых двух групп.

Файловые вирусы могут инфицировать:

- позиционно-независимые перемещаемые машинные программы находящиеся в COM-файлах;
- позиционно-зависимые перемещаемые машинные программы, размещаемые в EXE-файлах;
- драйверы устройств (SYS- и BIN-файлы);
- файлы с компонентами DOS;
- объектные модули (OBJ-файлы);
- файлы с программами на языках программирования (в расчете на компиляцию этих программ);
- командные файлы (BAT-файлы);
- объектные и символические библиотеки (LIB- и др. файлы);
- оверлейные файлы (OVL-, PIF- и др. файлы).

Наиболее часто файловые вирусы способны внедряться в COM и/или EXE-файлы.

Загрузочные вирусы могут заражать:

- загрузочный сектор на дискетах;
- загрузочный сектор системного логического диска, созданного на винчестере;
- внесистемный загрузчик на жестком диске.

Загрузочные вирусы распространяются на дискетах в расчете на то, что с них будет осуществлена попытка загрузиться, что происходит не так часто. У файловых вирусов инфицирующая способность выше.

Файлово-загрузочные вирусы обладают еще большей инфицирующей способностью, так как могут распространяться как в программных файлах, так и на дискетах с данными.

Способы заражения среды обитания, зависят от типа последней. Зараженная вирусом среда называется вирусоносителем. При имплантации тело файлового вируса может размещаться:

- в конце файла;
- в начале файла;
- в середине файла;
- в хвостовой (свободной) части последнего кластера, занимаемого файлом.

Наиболее легко реализуется внедрение вируса в конец COM-файла. При получении управления вирус выбирает файл-жертву и модифицирует его следующим образом:

1. дописывает к файлу собственную копию (тело вируса);
2. сохраняет в этой копии оригинальное начало файла;
3. заменяет оригинальное начало файла на команду передачи управления на тело вируса.

При запуске инфицированной описанным способом программы первоначально иницируется выполнение тела вируса, в результате чего:

1. восстанавливается оригинальное начало программы (но не в файле, а в памяти!);
2. возможно, отыскивается и заражается очередная жертва;
3. возможно, осуществляются несанкционированные пользователем действия;
4. производится передача управления на начало программы-вирусоносителя, в результате чего она выполняется обычным образом.

Имплантация вируса в начало COM-файла производится иначе: создается новый файл, являющийся объединением тела вируса и содержимого оригинального файла. Два описанных способа внедрения вируса ведут к увеличению длины оригинального файла.

Имплантация вируса в середину файла наиболее сложна и специализирована. Сложность состоит в том, что в этом случае вирус должен "знать" структуру файла-жертвы (например, COMMAND.COM), чтобы можно было внедриться, в частности, в область стека. Описанный способ имплантации не ведет к увеличению длины файла.

Проявлением (деструктивными действиями) вирусов могут быть:

- влияние на работу ПК;
- искажение программных файлов;
- искажение файлов с данными;
- форматирование диска или его части;
- замена информации на диске или его части;
- искажения системного или несистемного загрузчика диска;
- разрушение связности файлов путем искажения таблицы FAT;
- искажение данных в CMOS-памяти.

Большую часть вирусов первой группы, вызывающих визуальные или звуковые эффекты, неформально называют "иллюзионистами". Другие вирусы этой же группы могут замедлять работу ПК или препятствовать нормальной работе пользователя, модифицируя и блокируя функции выполняемых программ, а также операционной системы. Вирусы всех остальных групп часто называют "вандалами" из-за наносимого ими, как правило, непоправимого ущерба.

При повседневной работе пользователь в состоянии обнаружить вирус по его симптомам. Естественно, что симптомы вируса непосредственно определяются реализованными в нем способами проявления, а также др. характеристиками вируса. В качестве симптомов вирусов выделяют следующие:

- увеличение числа файлов на диске;
- уменьшение объема свободной оперативной памяти;
- изменения времени и даты создания файла;
- увеличение размера программного файла;
- появление на диске зарегистрированных дефектных кластеров;
- ненормальная работа программы;
- замедление работы программы;
- загорание лампочки дисководов в то время, когда к диску не должны происходить обращения;
- заметное возрастание времени доступа к жесткому диску;
- сбои в работе операционной системы, в частности, ее зависание;
- невозможность загрузки операционной системы
- разрушение файловой структуры (исчезновение файлов, искажение каталогов).

Наряду с компьютерными вирусами существуют и другие опасные программы, например, так называемые "черви", формально именуемые репликаторами. Их основная особенность состоит в способности к размножению без внедрения в другие программы. Репликаторы создаются с целью распространения по узлам вычислительной сети и могут иметь начинку, состоящую, в частности, из вирусов. В этом отношении можно провести аналогию между "червем" и шариковой бомбой.

Примером репликатора является программа ChristmasTree, рисующая на экране дисплея рождественскую елку, а затем рассылающая свои копии по всем адресам, зарегистрированным средствами электронной почты.

Классификация антивирусных средств

В настоящее время имеется большое количество антивирусных средств. Однако все они не обладают свойствами универсальности: каждое рассчитано на конкретные вирусы, либо перекрывает некоторые каналы заражения ПК или распространения вирусов. В связи с этим перспективной областью исследований можно считать применение методов искусственного интеллекта к проблеме создания антивирусных средств.

Антивирусным средством, называют программный продукт, выполняющий одну или несколько из следующих функций:

1. защиту файловой структуры от разрушения;
2. обнаружение вирусов;
3. нейтрализацию вирусов;

Вирус-фильтром (сторожем) называется резидентная программа, обеспечивающая контроль выполнения характерных для вирусов действий и требующая от пользователя подтверждения на производство действий. Контроль осуществляется путем подмены обработчиков соответствующих прерываний. В качестве контролируемых действий могут выступать:

- обновление программных файлов;
- прямая запись на диск (по физическому адресу);
- форматирование диска;
- резидентное размещение программы в ОЗУ.

Детектором называется программа, осуществляющая поиск вирусов как на внешних носителях информации, так и в ОЗУ. Результатом работы детектора является список инфицированных файлов и/или областей, возможно, с указанием конкретных вирусов, их заразивших.

Детекторы делятся на универсальные (ревизоры) и специализированные. Универсальные детекторы проверяют целостность файлов путем подсчета контрольной суммы и ее сравнения с эталоном. Эталон либо указывается в документации на программный продукт, либо может быть определен в самом начале его эксплуатации.

Специализированные детекторы настроены на конкретные вирусы, один или несколько. Если детектор способен обнаруживать несколько различных вирусов, то его называют полидетектором. Работа специализированного детектора основывается на поиске строки кода, принадлежащей тому или иному вирусу, возможно заданной регулярным выражением. Такой детектор не способен обнаружить все возможные вирусы.

Дезинфектором (доктором, фагом) называется программа, осуществляющая удаление вируса как с восстановлением, так и без восстановления среды обитания. Ряд вирусов искажает среду обитания таким образом, что ее исходное состояние не может быть восстановлено.

Наиболее известными полидетекторами-фагами являются программные пакеты AntiviralToolkitPro Евгения Касперского и DrWeb фирмы Диалог.

Иммунизатором (вакциной) называют программу, предотвращающую заражение среды обитания или памяти конкретными вирусами. Иммунизаторы решают проблему нейтрализации вируса не посредством его уничтожения, а путем блокирования его способности к размножению. Такие программы в настоящее время практически не используются.

Методы защиты от компьютерных вирусов

При защите от компьютерных вирусов как никогда важна комплексность проводимых мероприятий как организационного, так и технического характера. На переднем ее крае □ обороны □ целесообразно разместить средства защиты данных от разрушения, за ними □ средства обнаружения вирусов и, наконец, средства нейтрализации вирусов.

Средства защиты данных от возможной потери и разрушения должны использоваться всегда и регулярно. Дополнительно к этому следует придерживаться следующих рекомендаций организационного характера, чтобы избавиться от заражения вирусами:

- гибкие диски использовать всегда, когда это возможно, с заклеенной прорезью защиты от записи,
 - без крайней необходимости не пользоваться неизвестными дискетами;
 - не передавать свои дискеты другим лицам;
 - не запускать на выполнение программы, назначение которых не понятно;
- использовать только лицензионные программные продукты;
- ограничить доступ к ПК посторонних лиц.

При необходимости использования программного продукта, полученного из неизвестного источника, рекомендуется:

- протестировать программный продукт специализированными детекторами на предмет наличия известных вирусов. Нежелательно размещать детекторы на жестком диске
□ для этого нужно использовать защищенную от записи дискету.
- осуществить резервирование файлов нового программного продукта;
- провести резервирование тех своих файлов, наличие которых требуется для работы нового программного обеспечения;
- организовать опытную эксплуатацию нового программного продукта на фоне вирус-фильтра с обдуманными ответами на его сообщения.

Защита от компьютерных вирусов должна стать частью комплекса мер по защите информации как в отдельных компьютерах, так и в автоматизированных информационных системах в целом

Антивирус Касперского

Антивирус Касперского обеспечивает качественно новый уровень защиты вашего компьютера благодаря оптимальному сочетанию традиционных антивирусных технологий и современных проактивных методов.

Продукт легко установить и настроить, он предусматривает широкие возможности адаптации работы под индивидуальные потребности пользователей.

Программа отличается не только безупречной интеграцией с операционными системами семейства Microsoft Windows (в том числе Microsoft Windows x64), но и совместимостью с другими программными продуктами для защиты персональных компьютеров (например, сетевыми экранами).

Основные преимущества

- Высокая эффективность антивирусной защиты. Наряду с признанными «сигнатурными» технологиями, обеспечивающими традиционно высокое качество распознавания и лечения вирусов, в Антивирусе Касперского 6.0 применяются и новые проактивные технологии. Они обеспечивают защиту от вирусов на основе анализа процессов и поведения приложений на компьютере пользователя, а также позволяют полностью восстановить систему после вредоносного воздействия.

- Оптимизация для работы на мобильных ПК. Продукт позволяет использовать все основные преимущества ноутбуков, работающих на базе технологии Intel® Centrino™ для мобильных ПК: снижение энергопотребления при сохранении высокой производительности компьютера, использование беспроводных сетей Wi-Fi для автоматического обновления антивирусных баз. Также программа оптимизирована для работы на компьютерах с процессорами Intel®, поддерживающими технологию HT.

- Простота и удобство использования. Установка и первоначальная настройка Антивируса Касперского 6.0 занимают считанные минуты, а контекстная справочная система содержит исчерпывающую информацию по тонкой настройке приложения. Кроме этого, программа регулярно информирует пользователя о текущем статусе защищенности компьютера и дает рекомендации в случае неоднозначных ситуаций.

Ключевые характеристики

Антивирусная защита

- Защита электронной почты. Программа осуществляет антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ – Microsoft Outlook, Microsoft Outlook Express и TheBat! – предусмотрены плагины и лечение вирусов в почтовых базах.

- Проверка интернет-трафика. Антивирус Касперского 6.0 обеспечивает антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени, позволяя таким образом предотвратить заражение ещё до момента сохранения файлов на жестком диске компьютера.

- Защита файловой системы. Антивирусной проверке могут быть подвергнуты любые отдельные файлы, каталоги и диски. Кроме этого, используя предустановленную задачу

сканирования, можно запустить проверку только критических областей операционной системы и объектов, загружаемых при старте Windows. Это позволит сэкономить время, уделив внимание в первую очередь областям и объектам, которые обычно больше всего подвержены заражению.

Проактивная защита

- Контроль изменений в файловой системе. Антивирус Касперского 6.0 позволяет создать список приложений, компонентный состав которых будет контролироваться, что помогает предотвратить нарушение целостности приложений вредоносными программами.

- Наблюдение за процессами в оперативной памяти. Программа ведет наблюдение за деятельностью программ и процессов, запущенных в оперативной памяти компьютера и своевременно предупреждает пользователя в случае появления опасных, подозрительных или скрытых (rootkits) процессов, а также в случае несанкционированного изменения нормальных процессов.

- Мониторинг изменений в реестре операционной системы. Приложение контролирует состояние системного реестра и информирует пользователя при обнаружении подозрительных или попытках создания скрытых ключей в реестре.

- Блокирование опасных макросов. Проактивная защита позволяет контролировать работу макросов VisualBasicforApplications в документах MicrosoftOffice и блокировать выполнение опасных макрокоманд.

- Восстановление системы. В приложении реализована новая технология восстановления системы после вредоносного воздействия программ класса spyware: Антивирус Касперского 6.0 фиксирует все изменения реестра и файловой системы компьютера и может отменить их по решению пользователя.

Высокая скорость работы

- Технологии ускорения антивирусной проверки. Антивирус Касперского 6.0 отличается высокой скоростью работы благодаря заложенной в нем возможности проверять только новые и измененные файлы. Механизм приостановки антивирусного сканирования при увеличении пользовательской активности способствует оптимальному использованию вычислительных ресурсов компьютера.

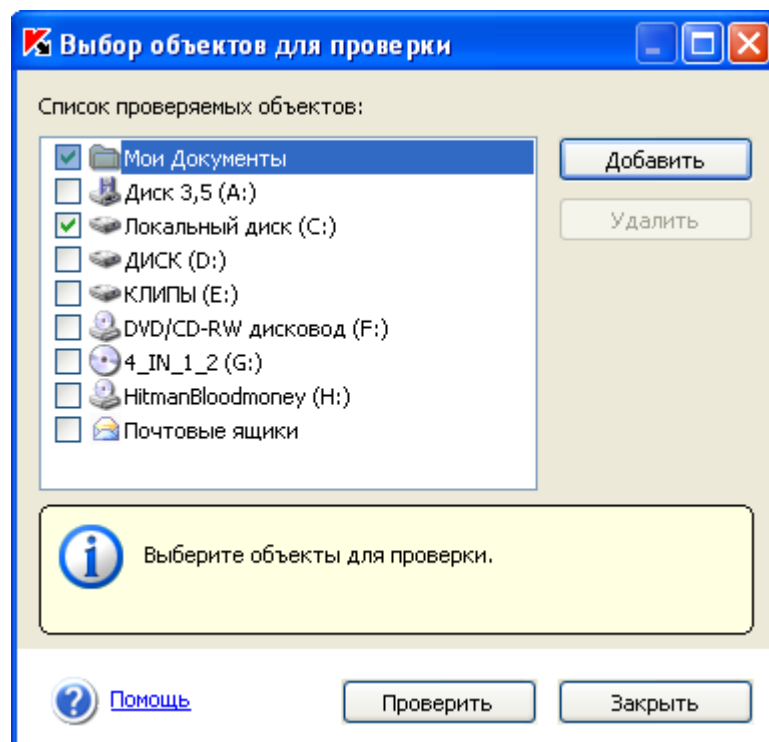
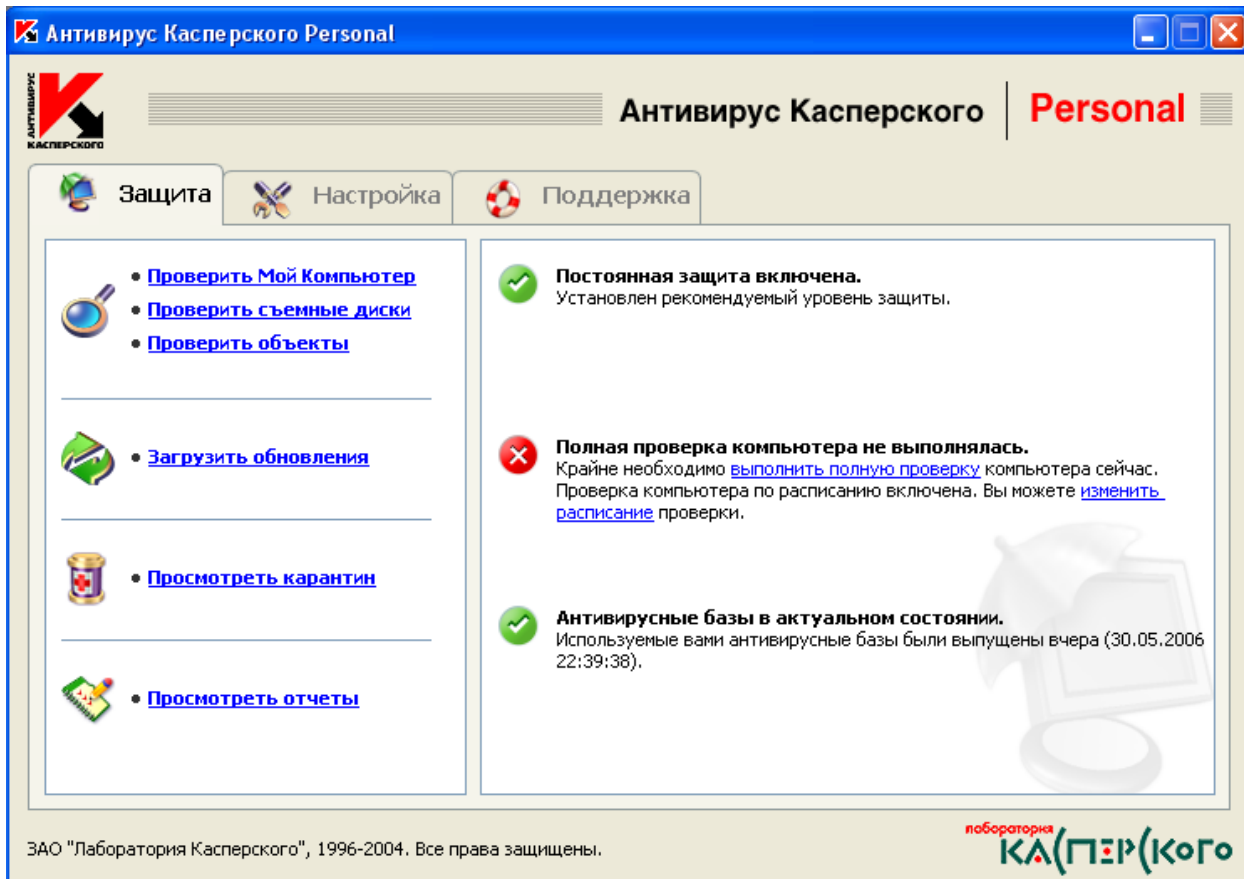
- Уменьшенный размер обновлений. По сравнению с предыдущей версией программы размер скачиваемых обновлений антивирусных баз уменьшился почти в 10 раз и обычно составляет несколько десятков килобайт, что обеспечивает практически мгновенное получение обновлений.

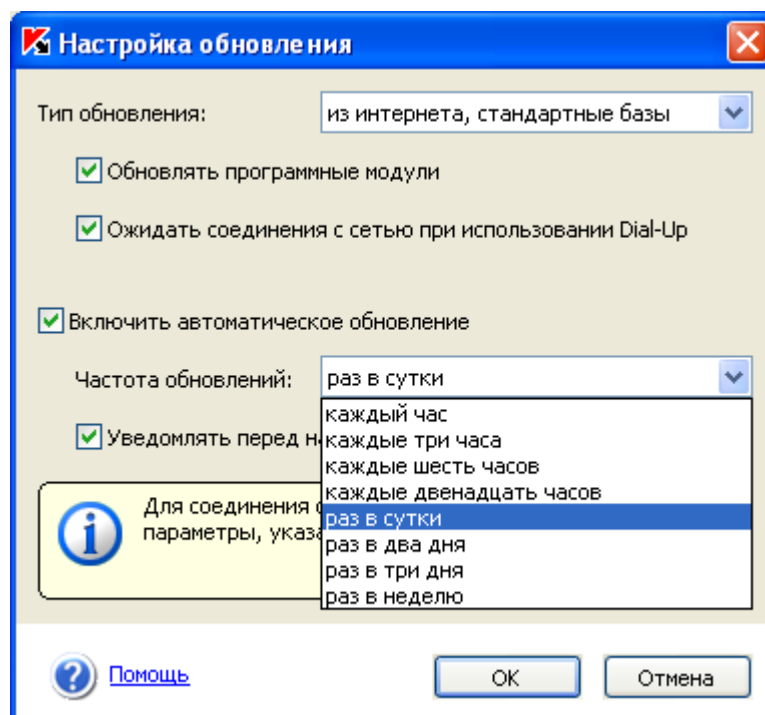
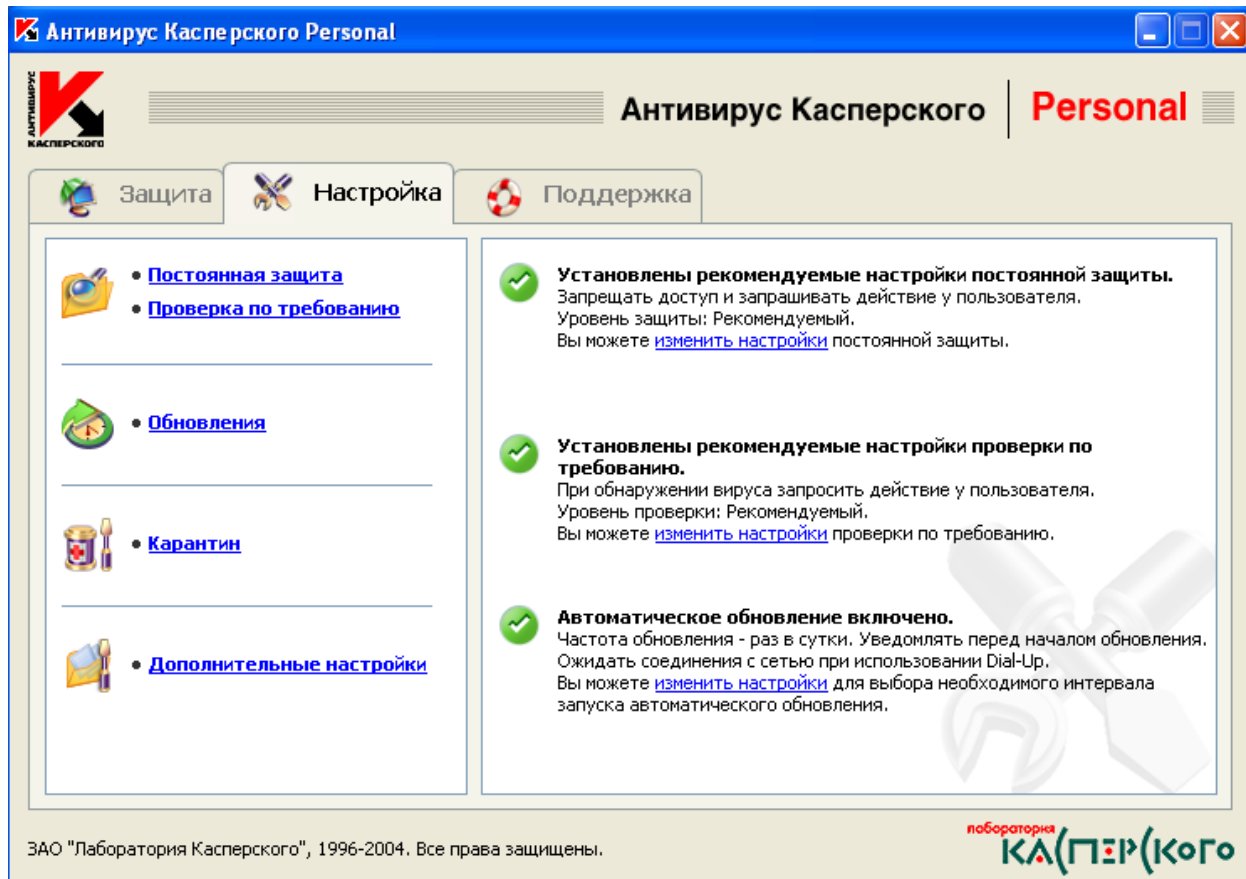
Системные требования

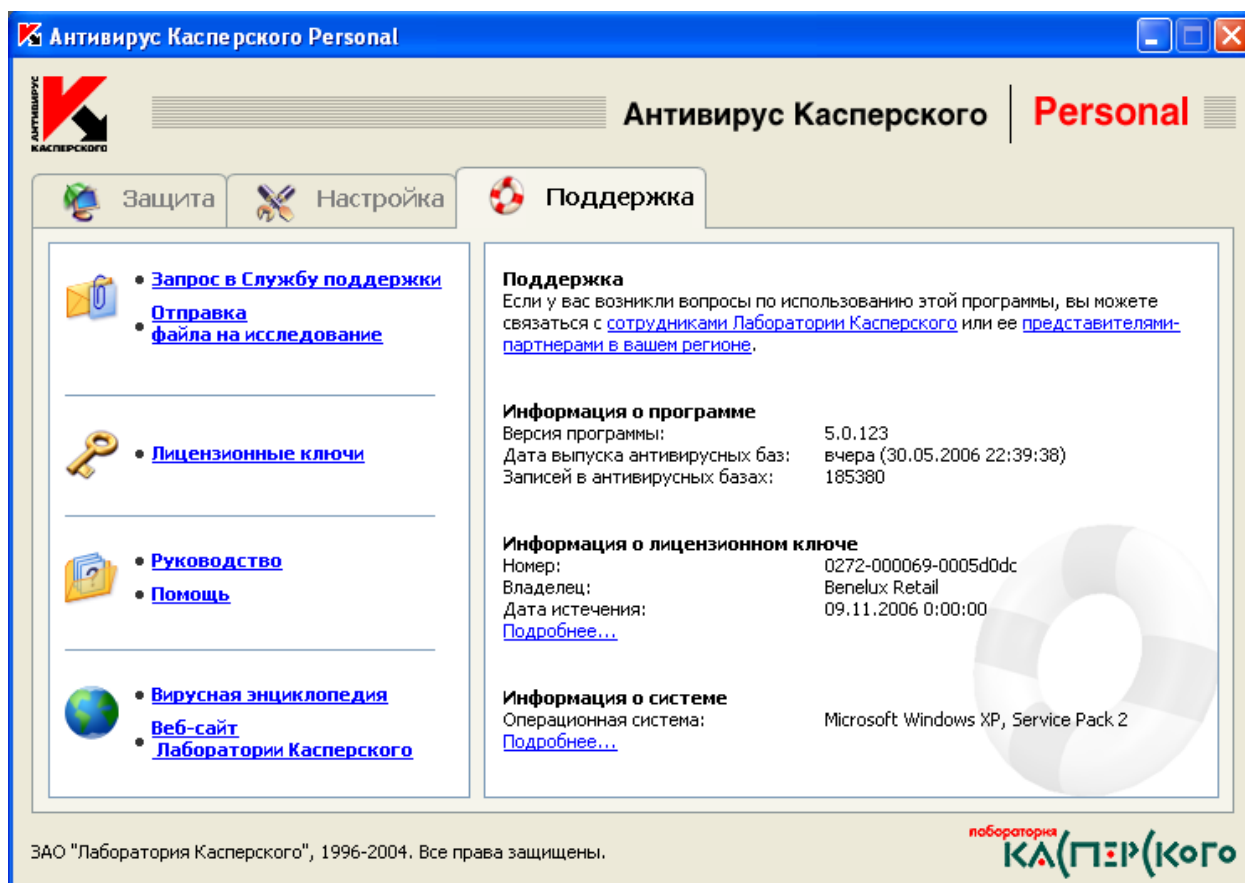
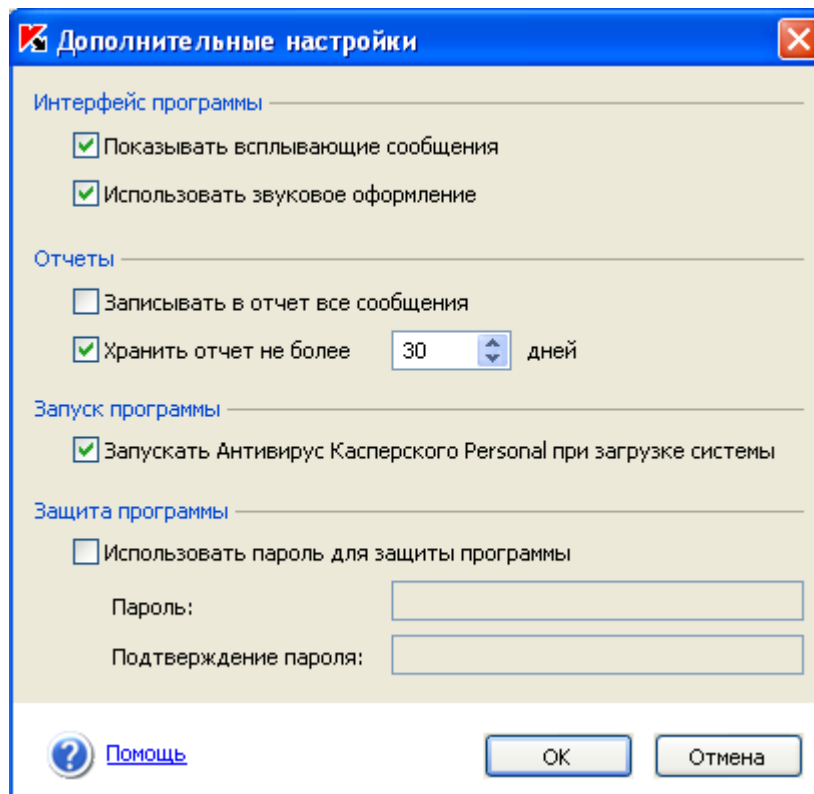
Общие требования	Аппаратные требования
Microsoft Windows 98 (SE) / NT Workstation 4.0	
<ul style="list-style-type: none"> - Microsoft Windows NT Workstation 4.0 (Service Pack 6a) - MicrosoftInternetExplorer 5.5 или выше (для обновления продукта и антивирусных баз через интернет) - CD-ROM (для инсталляции продукта с помощью CD) - Подключение к сети интернет (для активации продукта) 	<ul style="list-style-type: none"> - IntelPentium 133 MHz или выше - 32 MB RAM - 50 MB свободного пространства на жестком диске
MicrosoftWindows 2000 Professional	
<ul style="list-style-type: none"> - Microsoft Windows 2000 Professional (Service Pack 2 или выше) - MicrosoftInternetExplorer 5.5 или выше (для обновления продукта и антивирусных баз) 	<ul style="list-style-type: none"> - IntelPentium 133 MHz или выше - 64 MB RAM - 50 MB свободного пространства на жестком диске

<ul style="list-style-type: none"> - CD-ROM (для инсталляции продукта с помощью CD) - подключение к сети интернет (для активации продукта) 	
<ul style="list-style-type: none"> - MicrosoftWindows ME 	
<ul style="list-style-type: none"> - MicrosoftInternetExplorer 5.5 или выше (для обновления продукта и антивирусных баз) - CD-ROM (для инсталляции продукта с помощью CD) - подключение к сети интернет (для активации продукта) 	<ul style="list-style-type: none"> - IntelPentium 150 MHz или выше - 32 MB RAM - 50 MB свободного пространства на жестком диске
<p>Microsoft Windows XP Home Edition / XP Professional x64 Edition</p>	
<ul style="list-style-type: none"> - Microsoft Windows XP Home Edition (Service Pack 1 или выше) - MicrosoftInternetExplorer 5.5 или выше (для обновления продукта и антивирусных баз через интернет) - CD-ROM (для инсталляции продукта с помощью CD) - Подключение к сети интернет (для активации продукта) 	<ul style="list-style-type: none"> - IntelPentium 300 MHz или выше - 128 MB RAM - 50 MB свободного пространства на диске

Использование Антивируса Касперского на практике представлено на ниже перечисленных рисунках.







Тема № 4. Восстановление электронной информации.

Задание № 1 Восстановление зараженных файлов

Алгоритм выполнения работы Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий практически всю информацию из первоначальных документов и не содержащий макросы. Для этого выполните следующие действия.

1. В программе Word выберите пункты меню «Файл» — «Сохранить как».
2. В открывшемся окне в поле «Тип файла» выберите «Текст в формате RTF».
3. Выберите команду Сохранить, при этом имя файла оставьте прежним.
4. В результате появится новый файл с именем существующего, но с другим расширением.
5. Далее закройте Word и удалите все зараженные Word-документы и файл-шаблон NORMAL.DOT в папке WinWord.
6. Запустите Word и восстановите документы из RTF-файлов в соответствующий формат файла с расширением (.doc).
7. В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений. Примечание: а) этот метод рекомендуется использовать, если нет соответствующих антивирусных программ; б) при конвертировании файлов происходит потеря невирусных макросов, используемых при работе. Поэтому перед запуском описанной процедуры следует сохранить их исходный текст, а после обезвреживания вируса — восстановить необходимые макросы в первоначальном виде.
8. Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.
9. Для этого в Word выберите последовательно пункты меню: Сервис — Макрос — Безопасность.
10. В открывшемся окне на закладке Уровень безопасности отметьте пункт Высокая

Задание № 2 Защита программ и файлов от несанкционированного доступа

В настоящее время очень важно чтобы хранимая на компьютерах информация была защищена от несанкционированного к ней доступа и изменений. Существуют различные способы защиты информации и предотвращения их изменения: шифрование, кодирование, установка пароля. Возможна защита не только отдельных документов, но и даже папок и компьютеров полностью.

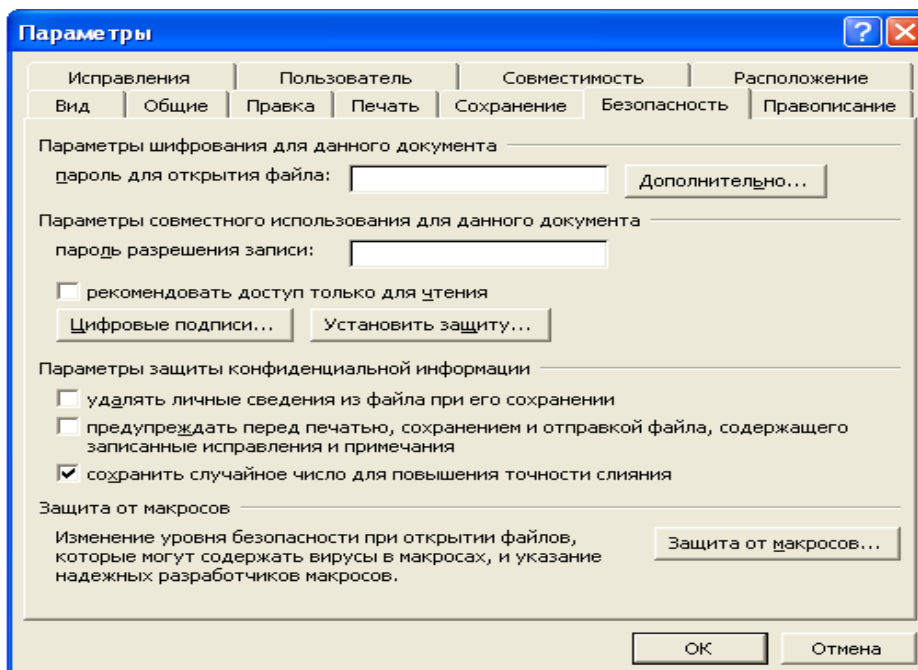
Можно ли установить пароль на доступ к информации и ее изменение во многом зависит от установленных на компьютере операционной и файловой систем. Так, например, пароль на компьютер можно установить только на те, на которых установлены операционные системы не старше Windows 2000 (Windows XP, Windows Millennium и др.). При этом стоит учитывать, что если будет установлена файловая система FAT 32, то будет не возможно установить пароли на папки со средствами Windows. Другая же не менее распространенная файловая система NTFS позволяет использовать различные способы защиты и предотвращения изменения информации.

Рассмотрим более подробно способы защиты папок и файлов от несанкционированного доступа, а также копирования, шифрования и изменения на примере операционной системы Windows XP и файловой системы NTFS.

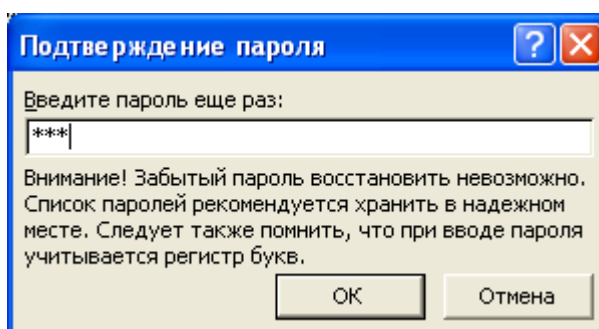
Пароль для доступа к информации в документах Word
(установка пароля, удаление информации о создателе документа).

Для того чтобы установить пароль на открытие файла надо сначала открыть сам документ. Потом в меню документа выбрать пункт СЕРВИС/ ПАРАМЕТРЫ. После этого на экране появится окно, на котором надо будет выбрать вкладку БЕЗОПАСНОСТЬ.

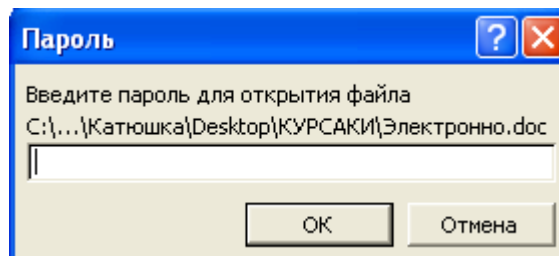
На ней в пункте ПАРОЛЬ ДЛЯ ОТКРЫТИЯ ФАЙЛА вводим пароль.



После этого на экране появится другое окно, в котором надо будет повторно ввести пароль.



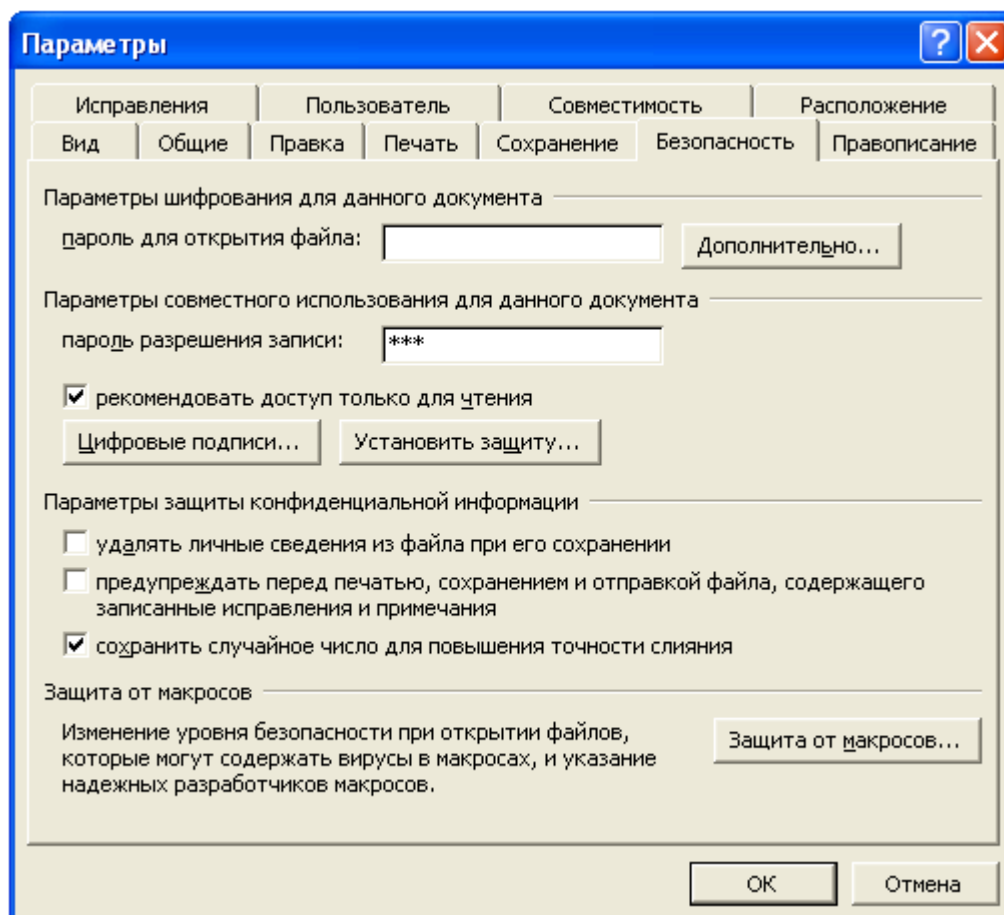
После этого нажмите кнопку ОК на каждом окне. После этого при открытии документа на экране будет появляться окно, в котором надо будет ввести пароль.



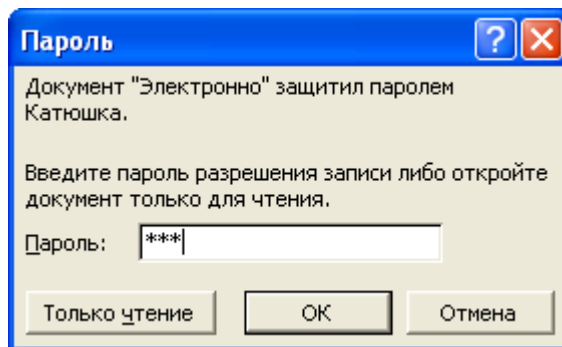
При неверно введенном пароле документ не будет открываться.

Защита документа от ввода данных, копирования, его удаления и печати.

Очень часто требуется, чтобы создаваемый документ использовался другими пользователями только для просмотра. Для этого надо открыть сначала сам документ. Потом пункт меню СЕРВИС/ПАРАМЕТРЫ. Появится окно. После этого надо выбрать вкладку БЕЗОПАСНОСТЬ, в которой установить пароль как рассказывалось выше в « Параметры совместного использования для данного документа» и поставить метку РЕКОМЕНДОВАТЬ ДОСТУП ТОЛЬКО ДЛЯ ЧТЕНИЯ. Это позволит спрашивать пользователя перед открытием документа, что он будет с ним делать: редактировать или только смотреть. В «параметры защиты конфиденциальной информации» поставить метку в пункте ПРЕДУПРЕЖДАТЬ ПЕРЕД ПЕЧАТЬЮ, СОХРАНЕНИЕМ И ОТПРАВКОЙ ФАЙЛА, СОДЕРЖАЩЕГО ЗАПИСАННЫЕ ИСПРАВЛЕНИЯ И ПРИМЕЧАНИЯ. После этого нажать кнопку ОК.



Теперь перед открытием документа будет появляться окно, в котором будет спрашиваться пароль, если вы хотите что-то сделать с документом. После ввода пароля надо нажать кнопку ОК. Если же вы хотите только посмотреть документ, то вам будет предложено нажать кнопку ТОЛЬКО ЧТЕНИЕ.



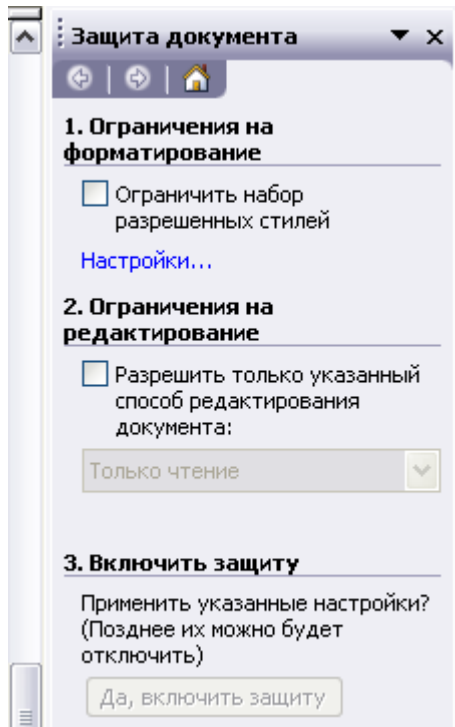
Стоит заметить, что если также установить пароль на сам документ полностью, то получится двойная защита. При этом первое появившееся окно будет запрашивать пароль на открытие самого документа, а второй, который будет вводиться в появившемся следом за этим окном, для определения действий, которые вы собираетесь совершать с документом.

Как снять защиту и удалить пароль?

Для того, чтобы удалить пароль и открыть полный доступ к документу надо открыть документ, на котором стоит пароль. После этого открыть пункт меню документа СЕРВИС/ПАРАМЕТРЫ. После открыть вкладку БЕЗОПАСНОСТЬ. На ней ПОБУКВЕННО (!) удалить нужные пароли. Если же удалить пароль целиком, то никакого фактического удаления не произойдет и запрос на введение пароля будет появляться снова.

Другие виды ограничений.

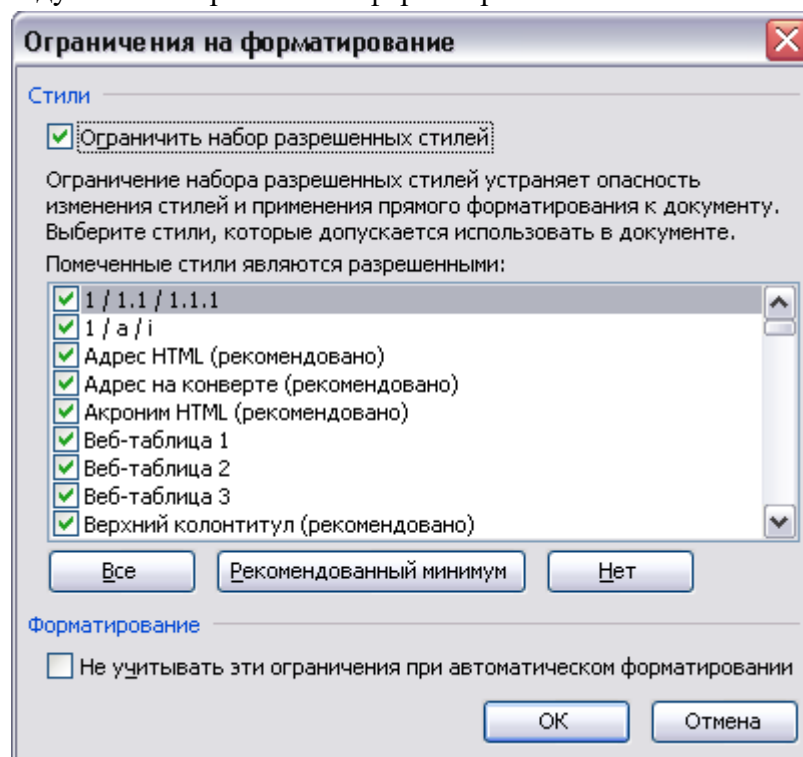
Помимо вышеуказанных ограничений можно установить и другие ограничения. Для этого надо открыть пункт меню документа СЕРВИС/ЗАЩИТА ДОКУМЕНТА. После этого в правом углу экрана появится меню, в котором будут указаны другие способы защиты документа.



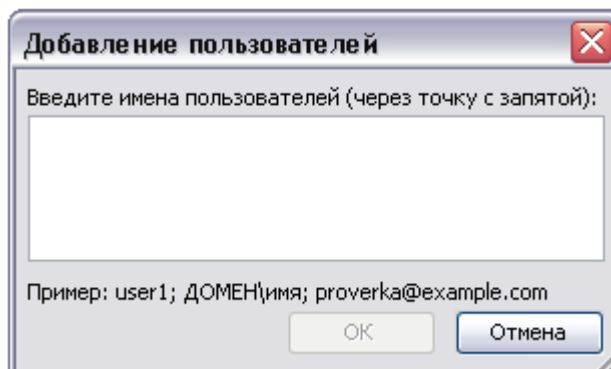
- ограничения на форматирование.
- ограничения на редактирования.

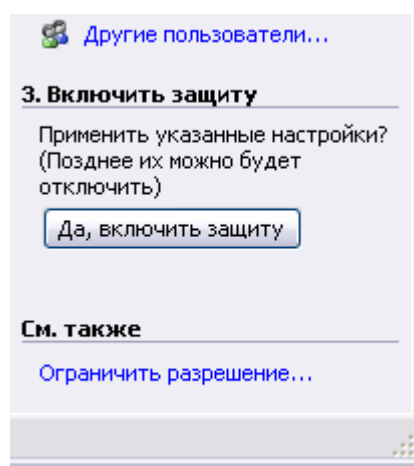
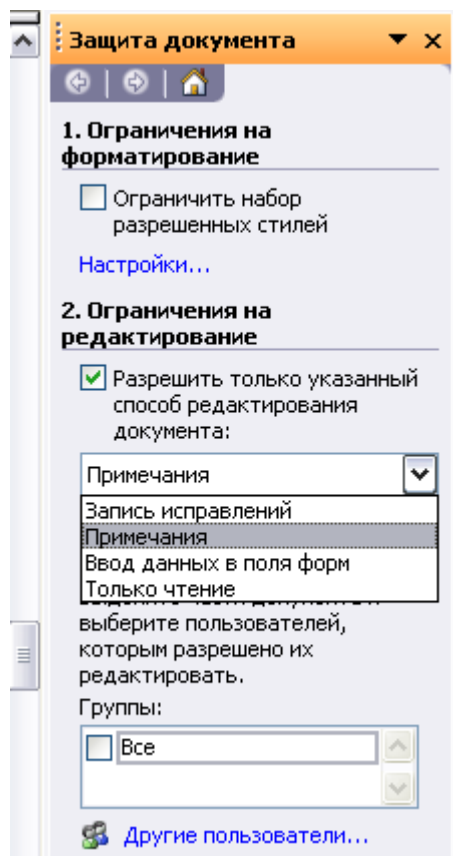
Если мы поставим галочку на пункте «Ограничить набор разрешенных стилей», то откроется другое меню. Ниже представлено это меню. При его появлении надо отметить пункт

«Ограничить набор разрешенных стилей». Это позволит самостоятельно выбрать те стили форматирования, которые будут допускаться при редактировании документа. Также после выделения вышеуказанного пункта активируется кнопка, при нажатии на которую система оставит только рекомендуемый набор способов форматирования.



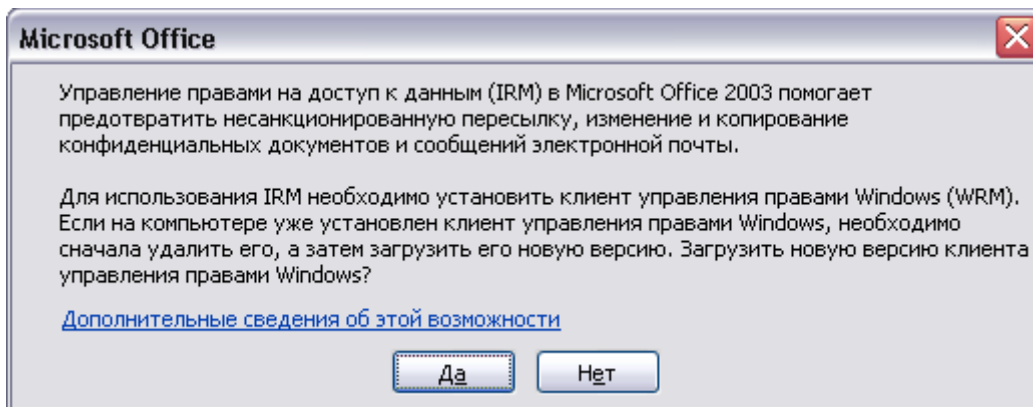
При выделении пункта «Разрешить только указанный способ редактирования документа». После этого можно будет указать только 1(!) какой-либо способ редактирования, а также указать пользователей, которым это можно делать. Если таких нет в представленном списке, то можно их добавить.





После выделения хотя бы одного из 2-х вышеуказанных пунктов появляется 3-й пункт, в котором надо подтвердить применение указанных ранее способов защиты текста.

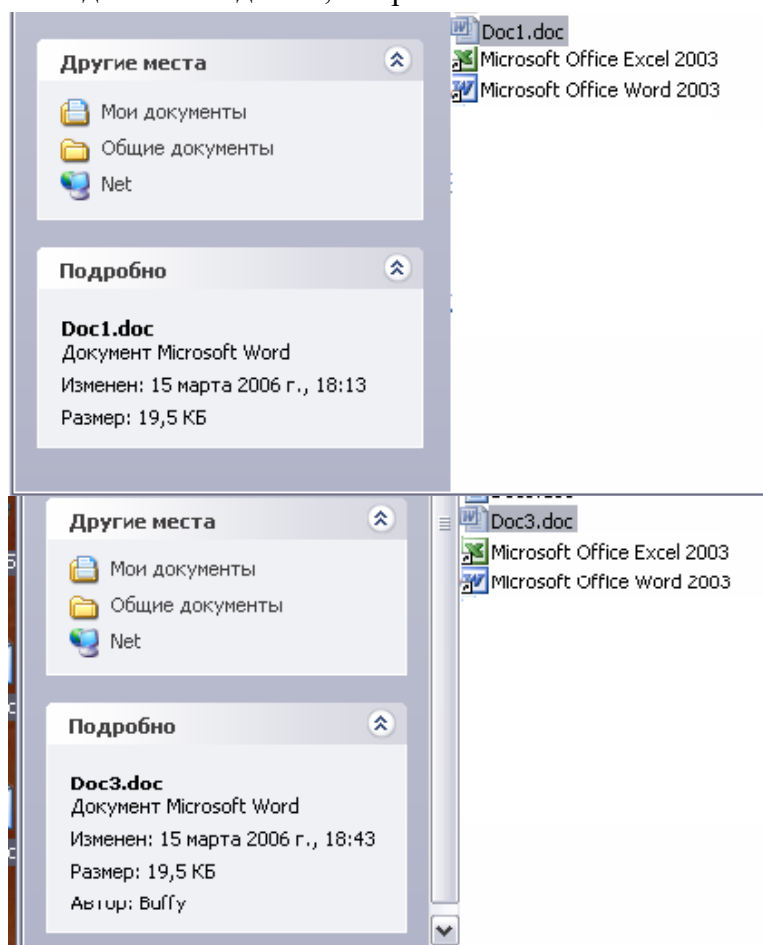
Как видно, открывается еще одна ссылка «ограничить разрешение», при вызове которой открывается окно, которое имеет ссылку для заключения договора с создателями операционной системы чтобы они прослеживали отправку документов с компьютера.



Также можно вызвать это окно и по другому пути: в меню документа выбрать **ФАЙЛ/РАЗРЕШЕНИЯ/НЕ РАСПРОСТРАНЯТЬ** или **ФАЙЛ/РАЗРЕШЕНИЯ /ОГРАНИЧИТЬ РАСРЕШЕНИЯ**.

Параметры защиты конфиденциальности.

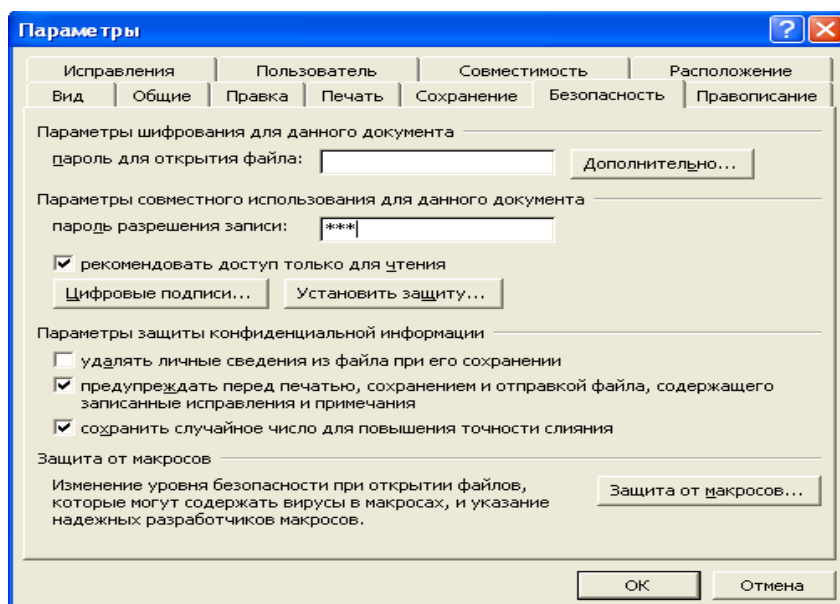
При сохранении компрометирующих документов важно, чтобы не были известны данные о создании этого документа. Для этого надо в пункте меню документа выбрать **СЕРВИС/ПАРАМЕТРЫ**. В появившемся окне поставить метку в «удалять личные сведения файла при сохранении документа». После этого при выделении документа не будет видно, кто создал документ. Внизу представлены два рисунка. Слева окно сведений о документе, в котором задано удаление сведений о создателе, а справа нет.



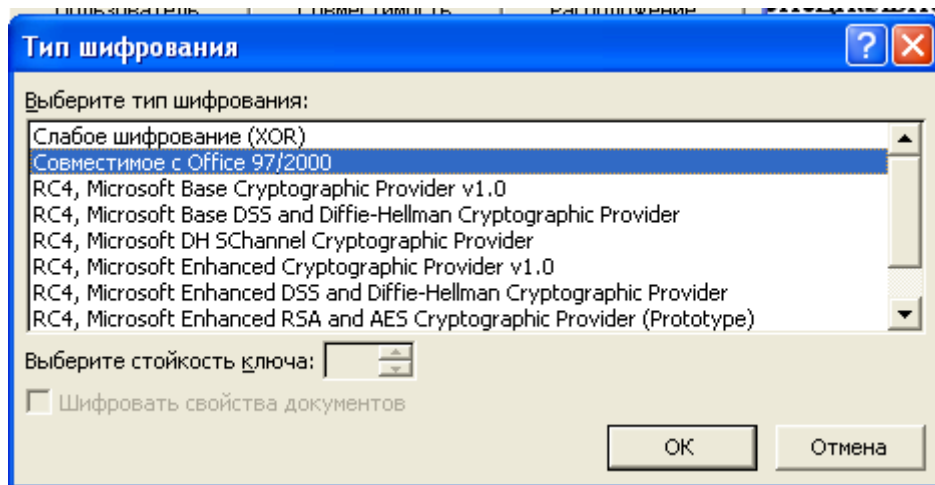
Стоит также отметить, что задание такого способа защиты надо задавать еще **ДО ПЕРВОГО СОХРАНЕНИЯ ДОКУМЕНТА**.

Шифрование документа.

Помимо ограничения доступа к самому документу можно зашифровать содержимое документа. Для этого надо выбрать в документе пункт меню СЕРВИС/ПАРАМЕТРЫ. После выбрать вкладку БЕЗОПАСНОСТЬ и там выбрать в «Параметры шифрования для данного документа». Там выбрать кнопку ДОПОЛНИТЕЛЬНО.



После этого появится окно, в котором надо выбрать тип шифрования.



После этого можно указать шифровать ли сведения с создателе документа и выбрать стойкость ключа. После нажать кнопку ОК.

Тема № 5. Электронный документооборот. Электронная цифровая подпись.

Задание № 1 Установите сертификат удостоверяющего центра и личный служебный сертификат с ключевого носителя.

Электронная цифровая подпись

В настоящее время бурно развиваются системы электронного документооборота, постоянно увеличивается объем документов, обрабатываемых в электронном виде. В системах

бумажного и электронного документооборота актуальными являются такие задачи как: • защита документов от модификации и подделки; • определение автора документа, а также подлинности документа; • обеспечение юридической силы документов; • защита документов от несанкционированного просмотра. В основе традиционных систем бумажного документооборота лежит принцип заверки документов подписью и печатью ответственного лица. Достоверность такого документа определяется визуально при его предъявлении. Степень защиты бумажных документов от различного рода угроз (подделка, дублирование и пр.) достаточна мала. В системах электронного документооборота для решения такого рода задач используются технологии Электронной Цифровой Подписи (ЭЦП). ЭЦП представляет собой небольшой объем информации, который добавляется к электронному документу. При получении или предъявлении документа, подписанного ЭЦП, можно легко установить его авторство и подлинность. Кроме того, ЭЦП защищает документ от модификации и подделки, так как содержит в себе сжатый и зашифрованный образ электронного документа – «дайджест» документа. Технологии электронной цифровой подписи базируются на криптографических алгоритмах с открытыми ключами (асимметричная криптография). На основе криптографических алгоритмов с открытыми ключами можно реализовать защиту информации при передаче по открытым каналам связи. Комплекс организационно-технических мероприятий и программно-аппаратных средств, необходимых для использования технологии с открытым распределением ключей называется – Инфраструктурой открытых ключей. Инфраструктура открытых ключей позволяет решать широкий спектр задач по защите информации в различных информационно-телекоммуникационных системах: электронный документооборот, сдача отчетности, медицина и телемедицина, платежные и трейдинговые системы.

Электронная цифровая подпись (англ. *digitalsignature*) – цифровой код (последовательность символов), присоединяемый к электронному сообщению для идентификации отправителя. По назначению электронная цифровая подпись соответствует обычной подписи на документе, подтверждающей юридические полномочия документа. Электронная цифровая подпись получается методами асимметричной криптографии, основанными на математической функции, комбинирующей открытый текст с последовательностью чисел (ключом). Алгоритм устроен таким образом, что пара «открытый ключ участника А – закрытый ключ участника Б» позволяет зашифровать сообщение, а пара «закрытый ключ А – открытый ключ Б» его дешифровать. Технология электронной цифровой подписи пересылаемого документа начинается с формирования его дайджеста (*digest*) – короткой последовательности чисел, восстановить исходный текст по которой нельзя. Любое изменение исходного документа вызовет его несоответствие дайджесту. К дайджесту добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой электронную подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.



Рис. 1. Технология электронной цифровой подписи

В целях повышения безопасности используют многократное шифрование блоков информации разными ключами.

В России, для обеспечения правовых условий использования электронной цифровой подписи в электронных документах, принят Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». Действие закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

Документ. Документооборот. Рассмотрим основные термины, относящиеся к документообороту. Документ — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Электронный документ — документ, в котором информация представлена в электронноцифровой форме. Документооборот — движение документов с момента их создания или получения до завершения исполнения, отправки адресату или передачи в архив. Делопроизводство — комплекс мероприятий по документационному обеспечению управления (ДОУ) организации, систематизации архивного хранения документов, обеспечению движения, поиска, хранения и использования документов. Архив — организация или ее структурное подразделение, осуществляющее прием и хранение документов с целью использования ретроспективной информации. Электронный архив — предназначен для систематизации архивного хранения электронных документов в рамках ДОУ. Документ в процессе своего жизненного цикла (ЖЦ) проходит определенные стадии:

- создание;
- визирование, согласование;
- подписание, утверждение;
- регистрацию;
- рассмотрение;
- исполнение;
- списание в дело;
- хранение, уничтожение.

Движение документов осуществляется в виде потоков циркулирующих между пунктами обработки информации и пунктами технической обработки документов. По отношению к аппарату управления потоками различают потоки входящих (поступающих), исходящих (отправляемых) и внутренних документов.

На этапе создания документ не имеет юридической силы и является проектом документа. Документ приобретает юридическую силу после оформления и удостоверения в установленном порядке. Электронный документ получает юридическую силу после его подписания электронной цифровой подписью (ЭЦП). Электронная цифровая подпись подтверждает, что содержательная информация документа не претерпела изменений с момента его подписания и документ подписан определенным лицом. При этом алгоритмы ЭЦП, а также механизмы и порядок применения ЭЦП должны соответствовать государственным нормативно-правовым требованиям. Системы электронного документооборота Развитие компьютерных технологий позволило во многих областях заменить бумажный документооборот безбумажным (электронным). Основные недостатки бумажного документооборота: • длительный поиск нужных данных и, как следствие, неоперативный доступ к необходимой информации; • возможность потери или порчи документа; • недостаточная конфиденциальность информации; • высокая вероятность подделки документа и/или реквизитов документа; • дублированный ввод информации; • учет документов требует дополнительных финансовых и трудовых затрат. Системы электронного документооборота (СЭД) позволяют решать проблемы бумажного документооборота. Первые системы электронного документооборота появились в банковской сфере. В западной литературе такие системы получили название " системы электронного перевода денежных средств" (The Electronic Funds Transfer Systems (EFTS)). Одна из таких систем SWIFT1 функционирует с начала 1970-х годов. В дальнейшем системы электронного документооборота стали широко применяться и для обмена другой коммерческой информацией (Английское название таких систем Electronic Data Interchange, или сокращенно EDI.). Уже много лет такие системы используются для продажи и бронирования авиационных билетов.

При использовании алгоритма с открытым ключом отпадает потребность в секретном канале связи для передачи ключа, т.к. открытый ключ не является секретной информацией. Различие ключей – открытого и закрытого – в криптографии с открытыми ключами позволило создать следующие технологии: • электронные цифровые подписи (задачи обеспечения целостности, авторства, актуальности информации, аутентификации субъекта и информации, неотказуемости); • распределенная проверка подлинности (задачи идентификации, аутентификации субъекта, авторизация доступа субъекта к информации); • согласование общего секретного ключа сессии (задачи обеспечения конфиденциальности информации при передаче по открытым каналам связи); • шифрование больших объемов данных без предварительного обмена общим секретным ключом (задачи обеспечения конфиденциальности информации). В настоящее время хорошо известен целый ряд алгоритмов шифрования с открытым ключом. Некоторые алгоритмы, например RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve

Cryptography), универсальны, они поддерживают все перечисленные выше операции. Другие алгоритмы более специализированы и поддерживают не все возможности. К числу алгоритмов шифрования с открытым ключом относятся: • российский алгоритмы электронной цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001; • алгоритм электронной цифровой подписи DSA (Digital Signature Algorithm, входящий в принятый в США государственный

стандарт цифровой подписи DigitalSignatureStandard, FIPS 186); • алгоритм DH (Diffie-Hellman), применяемый для выработки общего секретного ключа сессии.

Сертификаты открытых ключей В алгоритмах криптографии с открытыми ключами важным аспектом является определение принадлежности конкретного открытого ключа конкретному пользователю. В общем случае открытые ключи пользователей системы хранятся в общедоступном справочнике открытых ключей, и существует вероятность перехвата или подмены злоумышленниками открытого ключа какого-либо пользователя. Поэтому нужен механизм, который может обеспечить уверенность в том, что имеющийся открытый ключ принадлежит нужному пользователю, а не кому-либо другому. Один из таких механизмов основан на сертификатах открытых ключей, выдаваемых Удостоверяющими Центрами.



Рис. 4. Сертификат открытого ключа.

Сертификаты открытого ключа обеспечивают механизм надежной связи между открытым ключом и субъектом, которому принадлежит соответствующий закрытый ключ (см. рис.4). Сертификат – это цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью удостоверяющего центра выдавшего сертификат. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель (удостоверяющий центр) удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей (см. рис.5).



Рис. 5. Схема формирования сертификата открытого ключа.

В настоящее время наиболее часто используются сертификаты на основе стандарта Международного союза телекоммуникаций ITU-T X.509 v3 и рекомендаций ИETF (InternetEngineeringTaskForce) RFC 2459.

Удостоверяющий Центр - это служба, которая выдает сертификаты. Удостоверяющий Центр является гарантом связи между открытым ключом субъекта и содержащейся в сертификате информацией по идентификации этого субъекта. Различные УЦ устанавливают и гарантируют эту связь различными способами, поэтому прежде чем доверять сертификатам того или иного УЦ, следует ознакомиться с его политикой и регламентом. Удостоверяющие центры являются одной из основных составляющих ИОК. При построении ИОК в информационной системе с существенно распределенной структурой (например, организация с большим количеством подразделений или информационная система, объединяющая несколько организаций) встает задача построения и объединения в единую сеть нескольких Удостоверяющих центров. Наибольшее распространение получила иерархическую модель построения Удостоверяющих центров. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом коммерческих продуктов и УЦ различных поставщиков. Простейшая форма иерархии УЦ состоит из одного УЦ, а в общем случае – из множества УЦ с явно определенными отношениями родительский – дочерний (см. рис.6). В иерархической модели дочерние Удостоверяющие Центры сертифицируются родительским. Удостоверяющий центр, находящийся на самом верхнем уровне иерархии, обычно называется корневым. Подчиненные УЦ являются промежуточными или выдающими УЦ. Выдающим УЦ называется тот удостоверяющий центр, который выдает сертификаты конечным пользователям. Промежуточным УЦ называется тот УЦ, который не является корневым и выдает сертификаты только другим УЦ, а не конечным пользователям.

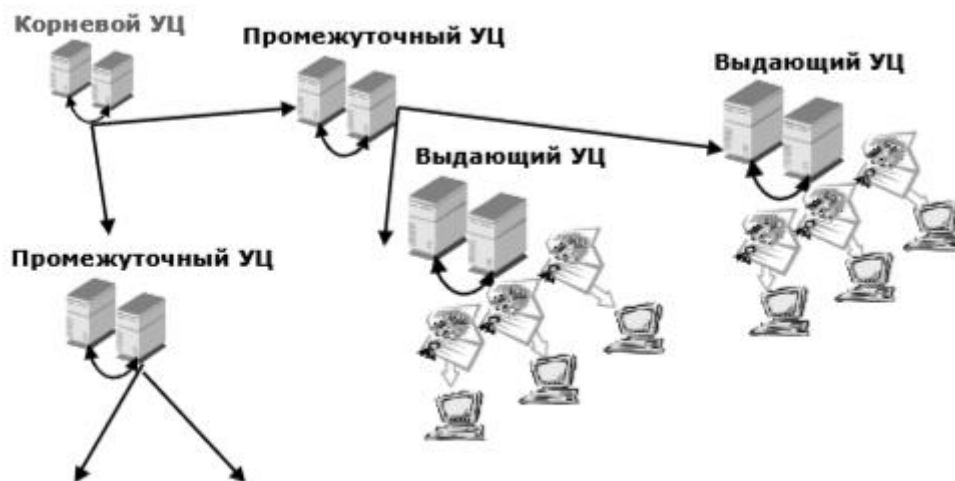


Рис. 6. Иерархическая модель объединения Удостоверяющих Центров.

Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых УЦ. В то же время эта модель позволяет иметь различное число УЦ, выдающих сертификаты. Списки отозванных сертификатов Удостоверяющие центры периодически выпускают списки отозванных сертификатов, в которых фиксируются сертификаты пользователей, вышедшие из обращения в системе.

Список отозванных сертификатов (CRL – CertificateRevocationList) – это цифровой документ, который содержит перечень сертификатов, являющихся отозванными из обращения

в УЦ. Удостоверяющий центр поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Абоненты могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов. Технологии на основе ИОК 1. Электронные цифровые подписи Одно из самых распространенных применений алгоритмов шифрования с открытыми ключами – электронная цифровая подпись (ЭЦП). Часто оказывается необходимым не зашифровывать содержимое электронного документа, а установить его авторство и подлинность. Основой электронной цифровой подписи является математическое преобразование подписываемых данных с использованием личного закрытого ключа подписывающего и выполнением следующих условий.

- Создать электронную цифровую подпись можно только с использованием личного закрытого ключа.
- Проверить действительность электронной цифровой подписи может любой, имеющий доступ к соответствующему открытому ключу.
- Любое изменение подписанных данных (даже изменение всего одного бита в большом файле) делает электронную цифровую подпись недействительной. При использовании цифровой подписи информация не шифруется и остается доступной любому пользователю, имеющему к ней доступ.

Процесс подписи документа Процесс подписи документа выглядит следующим образом. На первом шаге строится специальная функция (хэш-функция), напоминающая контрольную сумму, она идентифицирует содержимое документа (создается "дайджест" документа). На втором шаге автор документа шифрует содержимое хэш-функции своим персональным закрытым ключом. Зашифрованная хэш-функция помещается в то же сообщение, что и самодokument. Цифровая подпись является производной “дайджеста” и личного закрытого ключа, чем гарантируется её абсолютная уникальность (см. рис.7).

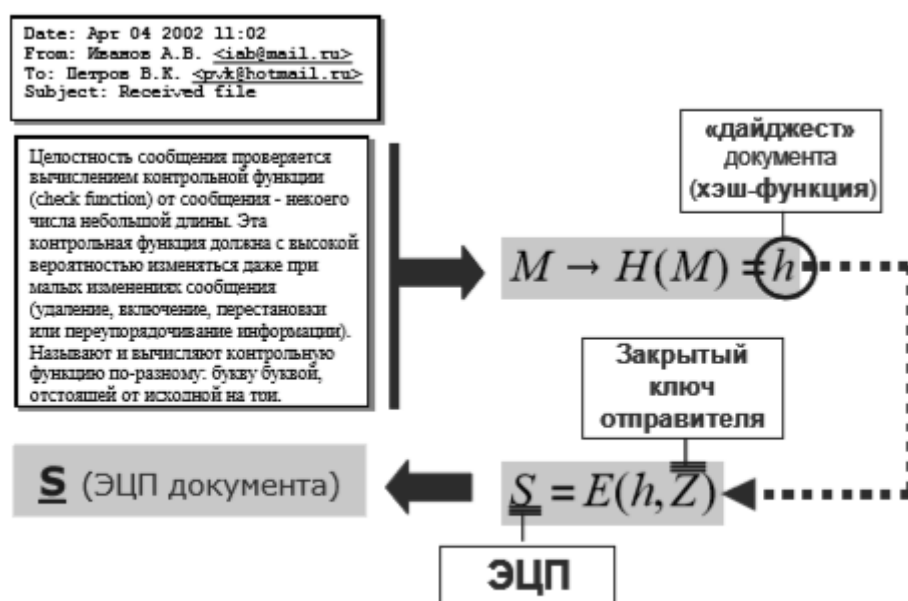


Рис. 7. Алгоритм формирования ЭЦП.

Используемая в алгоритме ЭЦП хеш-функция должна удовлетворять ряду требований, а именно:

- сообщение любой длины должно преобразовываться в бинарную последовательность фиксированной длины;
- полученная хешированная версия сообщения должна зависеть от каждого бита исходного сообщения и от порядка их следования;
- по хешированной версии сообщения нельзя никакими способами восстановить само сообщение.

Алгоритм верификации электронной подписи Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный

вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш-функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (см. рис.8).



Рис. 8. Алгоритм верификации ЭЦП.

Электронную цифровую подпись, как и любые другие данные, можно передавать вместе с подписанными, то есть защищенными ею данными. Кроме того, цифровая подпись позволяет убедиться в том, что данные при передаче адресату не были изменены (случайно или преднамеренно). Шифрование и электронная подпись могут с успехом применяться вместе. Сначала можно подписать документ личным закрытым ключом, а потом зашифровать открытым ключом адресата. Подпись удостоверяет личность, шифрование защищает письмо от чужих глаз.

В операционных системах семейства MS Windows присутствуют специальные криптографические модули для работы с симметричной и асимметричной криптографией. Приложения, использующие криптографические модули операционной системы, функционируют в соответствии с программным интерфейсом CryptoAPI, описывающим стандартные процедуры взаимодействия высокоуровневого приложения с низкоуровневыми криптографическими модулями. В базовый пакет ОС MS Windows входят приложения, такие как MS OutlookExpress и MS InternetExplorer, позволяющие использовать Инфраструктуру Открытых Ключей в технологиях электронной почты и WEB. В ОС MS Windows может присутствовать большое количество сертификатов открытых ключей (сертификаты корневых УЦ, сертификаты промежуточных УЦ, сертификаты других пользователей, личные сертификаты и т.д.). Сертификаты организованы в виде хранилищ в соответствии с категорией владельца сертификата. В ОС MS Windows для поддержки криптографическими модулями российских криптоалгоритмов необходимо установить дополнительное криптографическое программное обеспечение (криптографическое ядро) сторонних разработчиков. В соответствии с российскими государственными нормативно-правовыми требованиями криптографическое ядро должно быть сертифицировано уполномоченными государственными органами. Одним из наиболее распространенных криптографических ядер, реализующих российские криптоалгоритмы, является средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», разработанное фирмой «Крипто-Про». Данное криптоядро позволяет приложениям взаимодействовать через стандартный интерфейс CryptoAPI с криптографическими модулями, реализующими российские криптоалгоритмы. Основные сервисные функции СКЗИ «КриптоПро CSP» Доступ к настройкам СКЗИ можно

получить используя пункты меню Пуск, Настройка, Панель управления в окне панели управления выберите значок КриптоПро CSP. Модуль управления КриптоПро CSP представлен в виде нескольких вкладок, объединенных в соответствии с функциональным назначением.

Вкладка Общие – информация о версии ПО и ввод лицензии. • Вкладка Оборудование – управление ключевыми носителями (добавление, удаление, конфигурирование) и датчиками случайных чисел. • Вкладка Безопасность – настройка правил хранения и обращения ключей на локальном компьютере. • Вкладка Дополнительно – настройка времени ожидания ввода. • Вкладка Алгоритмы – настройка криптоалгоритмов. • Вкладка Сервис – сервисные функции работы с ключевыми контейнерами и сертификатами. Подробную информацию по сервисным функциям можно найти в руководстве пользователя СКЗИ КриптоПро.

1. Ключевой контейнер При формировании закрытые ключи записываются на ключевой носитель (в ключевой контейнер). Ключевой контейнер может содержать: • только ключ подписи; • только ключ шифрования; • ключ подписи и ключ шифрования одновременно. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т.п. Каждый контейнер (независимо от типа носителя), является полностью самостоятельным и содержит всю необходимую информацию для работы, как с самим контейнером, так и с закрытыми (соответствующими им открытыми) ключами. Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а так же вместе с личными ключами пользователя на ключевом носителе. При этом сертификат может храниться в виде записей в ключевом контейнере или в виде отдельного файла. Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места. В процессе работы с ключами (генерация ключей, использование в процедурах формирования подписи, аутентификации и шифрования), имеется возможность установки на ключевой контейнер дополнительного средства защиты ключевого контейнера - пароля (ПИН-кода). Сменить пароль на ключевой контейнер можно в настройках КриптоПро вкладка «Сервис», кнопка «Изменить пароль».

2. Использование ключей и сертификатов на компьютере Для того, чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальный справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя. В окне модуля управления КриптоПро CSP перейдите на вкладку Сервис. Если сертификат пользователя интегрирован в ключевой контейнер, то нажмите кнопку «Просмотреть сертификаты в контейнере» и следуйте указаниям мастера. Ключевой носитель, содержащий личный ключ и сертификат, при этом должен быть вставлен в соответствующее устройство считывания. Если на ключевом носителе содержится сертификат, его содержание будет отображено в стандартном окне просмотра сертификатов. Нажмите кнопку «Установить сертификат» для его переноса с ключевого носителя в локальный справочник. Если сертификат пользователя находится на ключевом носителе в виде отдельного файла, то воспользуйтесь мастером «Установить личный сертификат». Менеджмент сертификатов на локальном компьютере В ОС MS Windows присутствуют встроенные средства управления сертификатами открытых ключей (добавление, удаление, перенос, просмотр и пр.) такие как менеджер сертификатов (реализовано начиная с MS Windows 95) и консоль управления сертификатами (начиная с MS Windows 2000). Установить сертификаты из файлов (тип файлов .cer и .p7b) можно выбрав в контекстном меню файла пункт Установить сертификат.

Для запуска приложения «Менеджер сертификатов» нужно открыть Свойства обозревателя (в панели управления или в Internet Explorer), вкладка Содержание, кнопка Сертификаты. Менеджер отображает содержимое хранилищ сертификатов, доступных для данного пользователя и позволяет выполнять различные операции с сертификатами.

Для формирования консоли управления сертификатами создайте пустую консоль (команда mmc), добавьте в консоль оснастку управления сертификатами (меню Консоль -> Добавить или удалить оснастку -> кнопка Добавить -> оснастка Сертификаты). Консоль позволяет управлять сертификатами в хранилищах доступных для локального компьютера и/или пользователя. Отображаются все хранилища сертификатов присутствующие в ОС.

Функции ЭЦП и шифрования в MS Outlook Express Программное обеспечение Outlook Express версии 5.0 и выше полностью поддерживает Инфраструктуру Открытых Ключей для обеспечения конфиденциальности, целостности авторства почтовых сообщений, передаваемых по протоколам SMTP, IMAP, POP3. Для этих целей Outlook Express использует функции CryptoAPI 2.0 и сертификаты открытых ключей X.509. В качестве формата защищенных сообщений используется формат, описанный в рекомендациях SecureMultipurposeInternetMailExtensions (S/MIME).

1. Конфигурация Outlook Express Для создания или редактирования учетных записей электронной почты выберите Сервис, Учетные записи и нажмите на закладку Почта. Для создания новой учетной записи нажмите Добавить, Почта. Для редактирования учетной записи в списке учетных записей, выберите ту, которую необходимо настроить и нажмите кнопку Свойства. Для настройки использования ЭЦП выберите закладку Безопасность в отображаемом диалоге. Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для формирования электронной цифровой подписи и расшифрования входящих сообщений. В диалоге выбора сертификат отображаются только сертификаты, имеющие совпадающий адрес электронной почты и разрешенные для защиты электронной почты. В меню Сервис, Параметры на вкладке Безопасность можно включить режимы автоматического шифрования и ЭЦП каждого сообщения. Если эти режимы не включены, опции шифрования и подписи нужно будет включать для каждого отправляемого сообщения. Кнопка Дополнительно вызывает окно с настройками отправки и проверки сертификатов.

2. Отправка подписанных сообщений Для создания и отправки подписанного сообщения нажмите кнопку Создать сообщение или выберите пункт меню Файл, Создать, Сообщение. Заполните необходимые поля письма. Для отправки сообщения в подписанном виде проверьте что кнопка Подписать нажата и виден признак подписанного сообщения в правой части экрана. Нажмите кнопку Отправить.

3. Шифрование сообщений Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать подписанное сообщение в адрес требуемого абонента (сообщение посылается вместе с сертификатом отправителя). После получения сообщения и проверки электронной цифровой подписи производится добавление (автоматическое или нет) адресата отправителя и его сертификата в адресную книгу. Для отправки зашифрованного сообщения в окне создания сообщения нажмите кнопку Шифрование, появится признак шифрованного сообщения в правой части экрана. Шифрованное сообщение можно подписать ЭЦП нажав кнопку Подписать.

Удостоверяющий центр КриптоПро Основные компоненты программно-аппаратного комплекса Удостоверяющий центр КриптоПро: • Центр сертификации (ЦС) • Центр регистрации (ЦР) • Автоматизированное рабочее место (АРМ) администратора • АРМ пользователя Центр сертификации предназначен для формирования сертификатов открытых ключей пользователей

и администраторов Удостоверяющего центра, списков отозванных сертификатов, хранения эталонной базы сертификатов и списков отозванных сертификатов. ЦС взаимодействует только с Центром регистрации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. Центр регистрации предназначен для хранения регистрационных данных пользователей, запросов на сертификаты и сертификаты пользователей, предоставления интерфейса взаимодействия пользователей и Удостоверяющего центра. ЦР взаимодействует с ЦС по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. Взаимодействие пользователей с Удостоверяющим центром обеспечивается за счет использования АРМ пользователя, предоставляемого ЦР пользователю.

Вариант 1. Устанавливаем корневой сертификат УЦ, выдавшего ЭЦП

Как установить сертификат ЭЦП — вопрос, волнующий многих пользователей, оплативших ключ ЭЦП. Перед тем как непосредственно перейти к делу, необходимо скачать программу «КриптоПро» с официального сайта.

Установка сертификата ЭЦП допустима двумя путями:

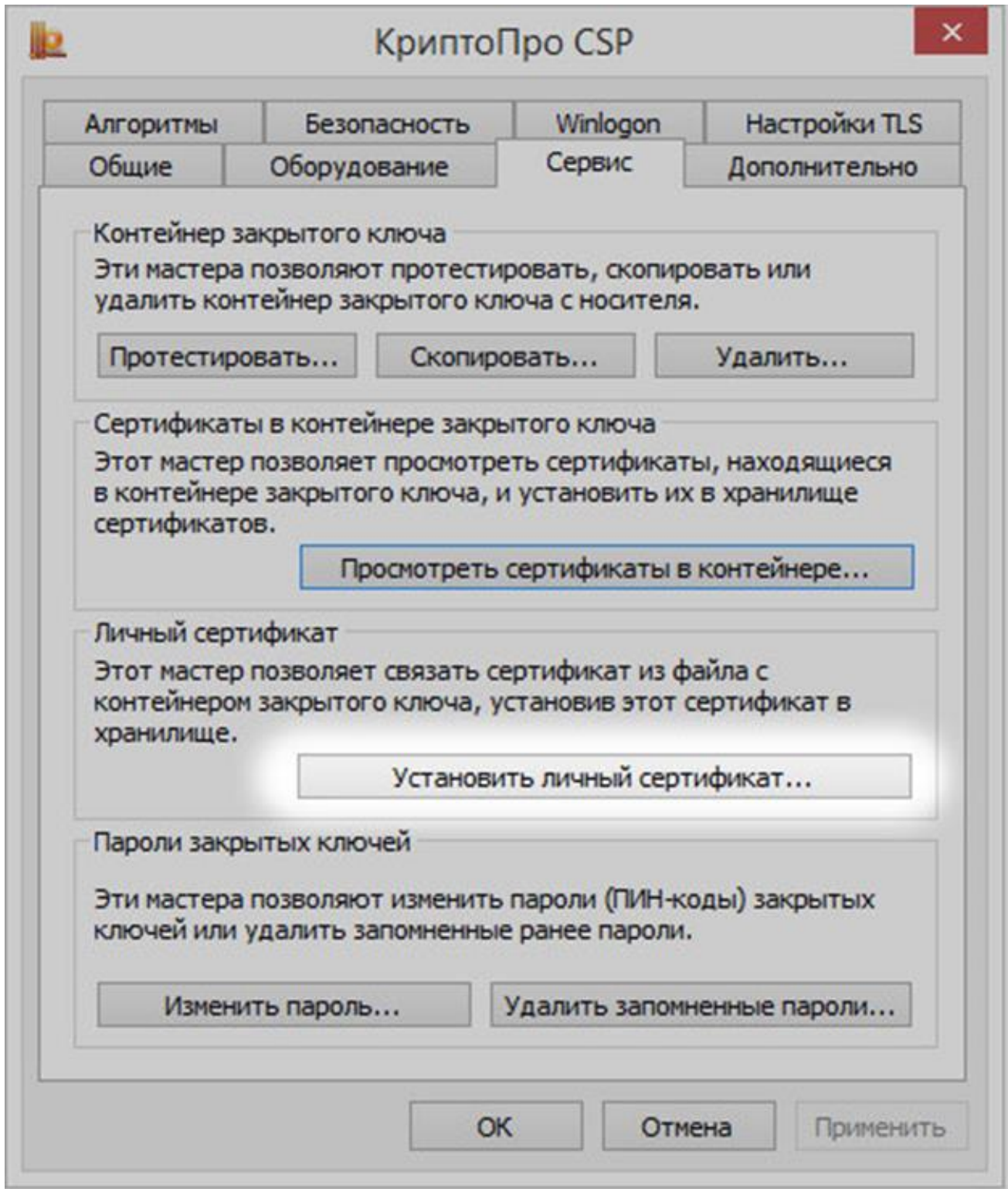
используя раздел «Установить личный сертификат»;

используя раздел «Просмотреть сертификаты в контейнере».

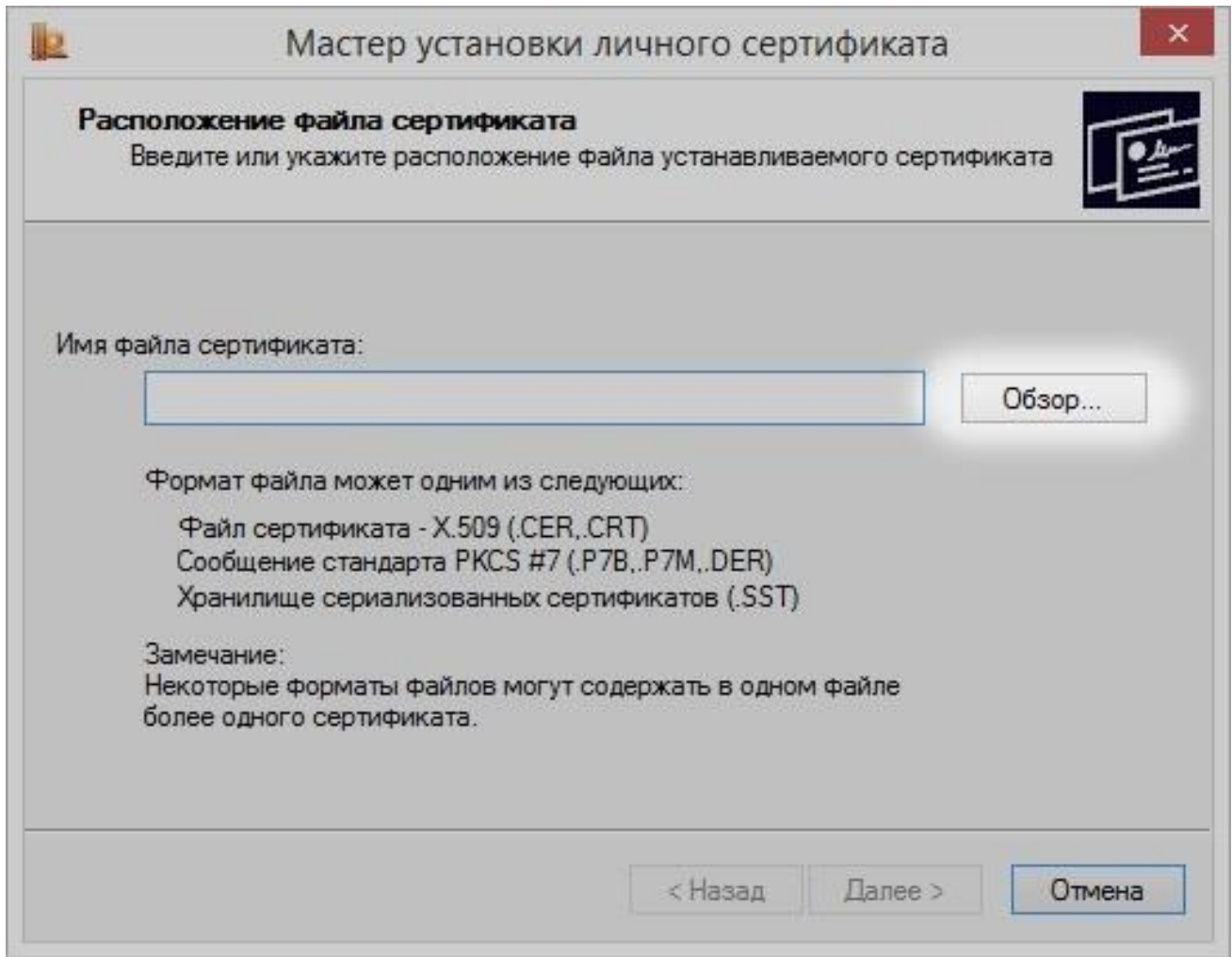
Рассмотрим первый случай более подробно.

В строке управления находим программу «КриптоПро CSP» и открываем ее.

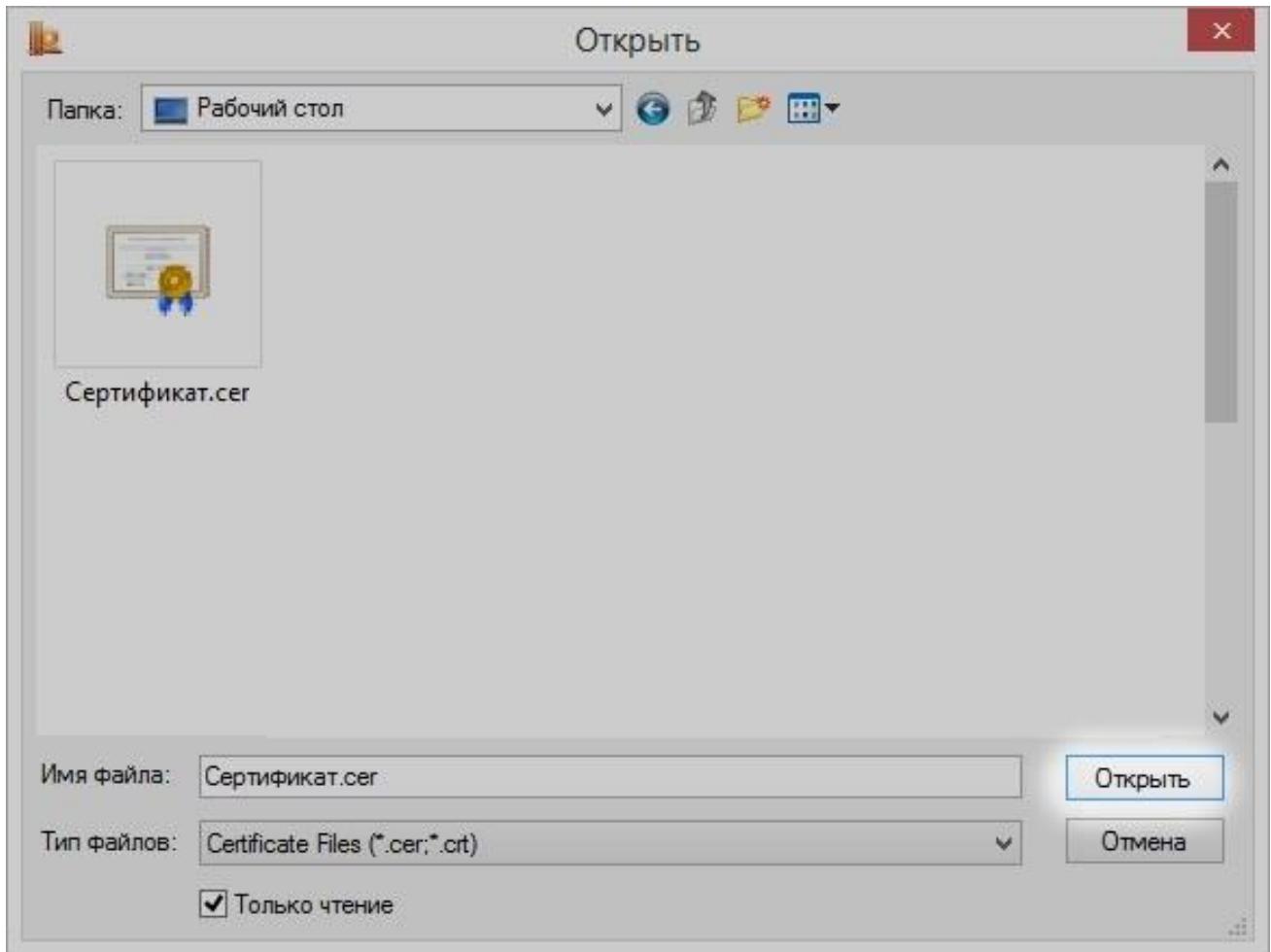
Переходим на закладку «Сервис» и находим клавишу «Установить личный сертификат».



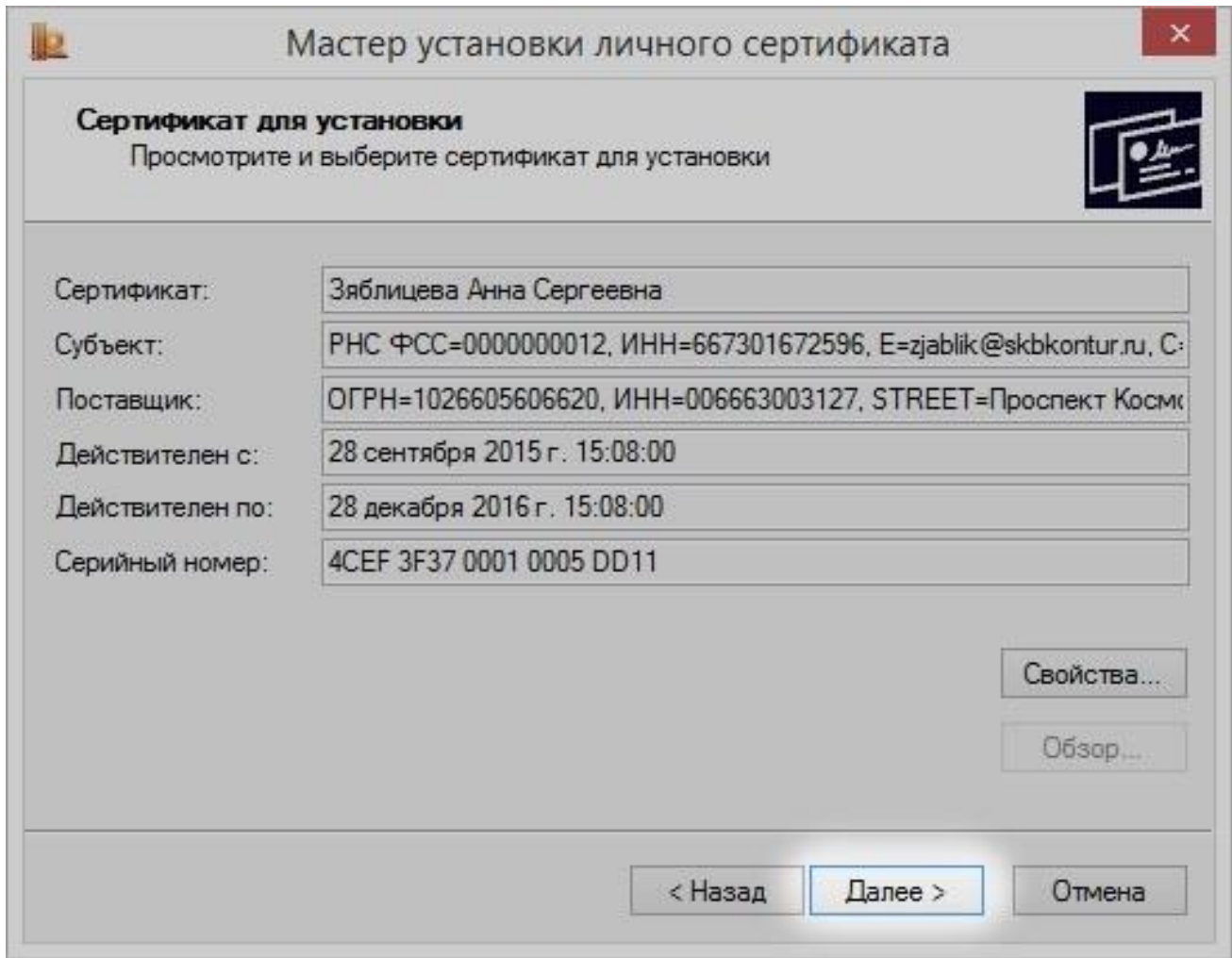
В ответ откроется окошко «Мастер установки сертификатов» — жмем «Далее». Кнопкой «Обзор» прокладываем путь к сертификату



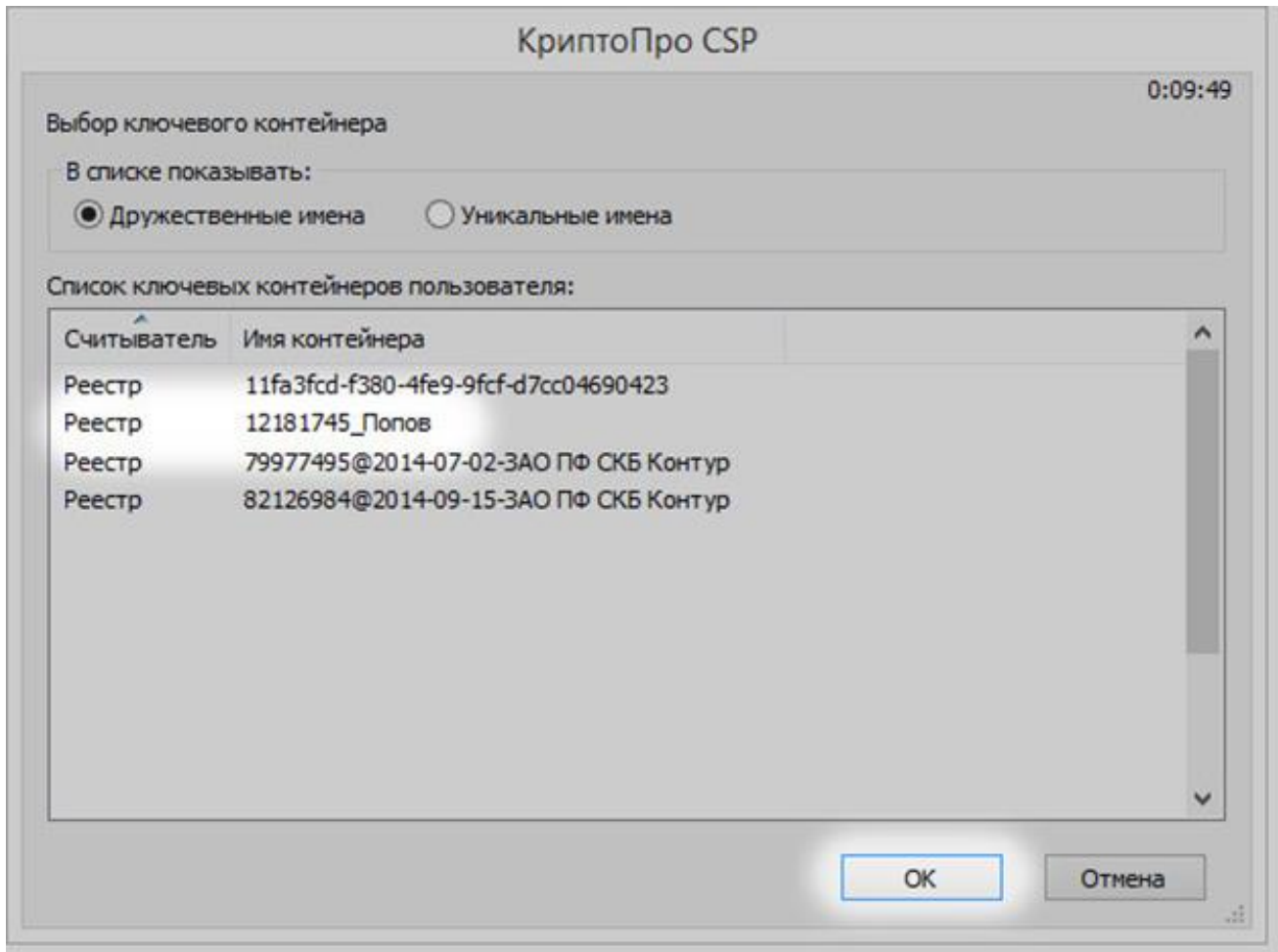
и переходим к клавише «Открыть».



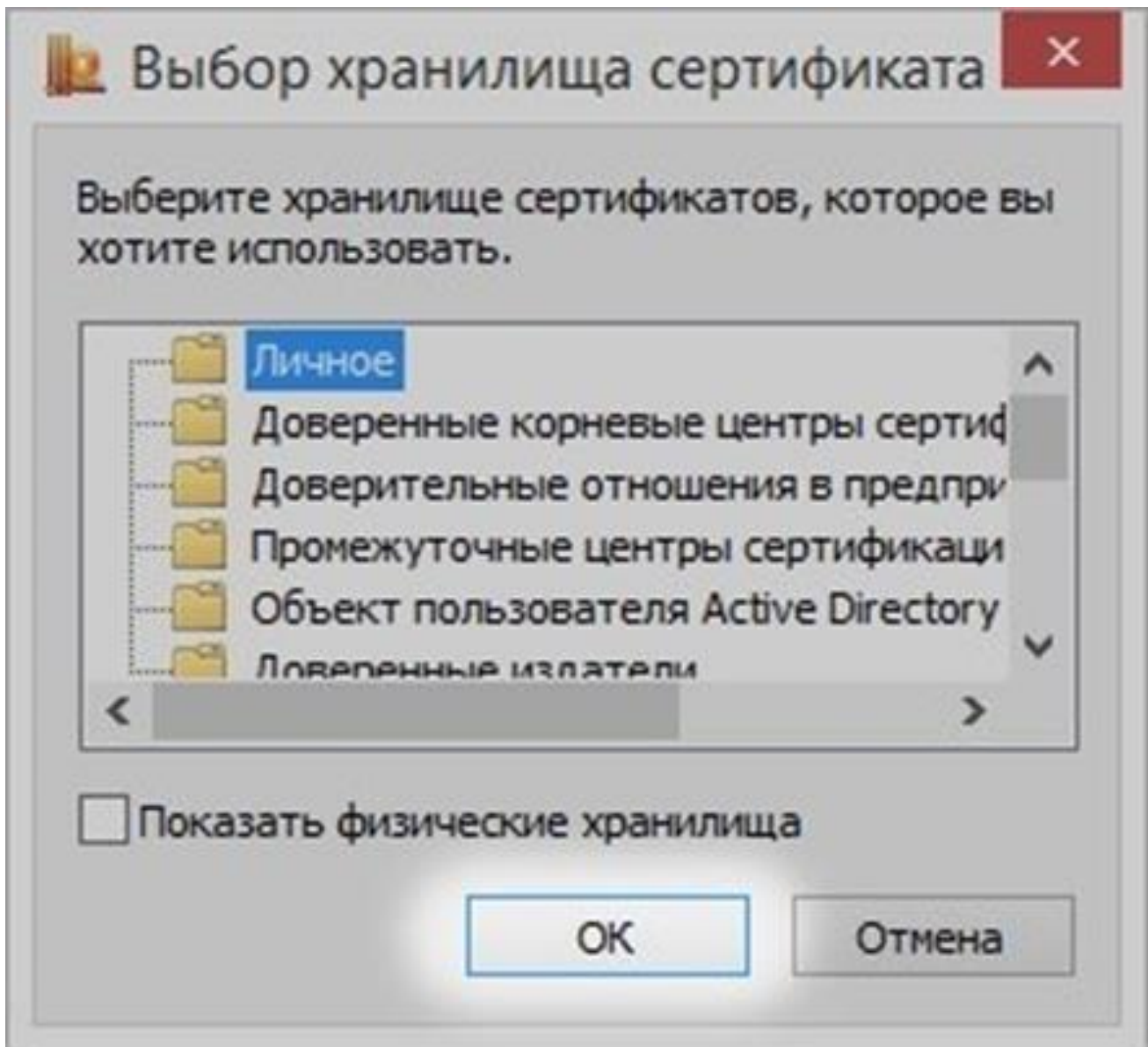
В открывшемся окошке находим кнопку «Далее».



Кликаем «Обзор» и в новом окне подбираем соответствующий сертификату контейнер — жмем «ОК».



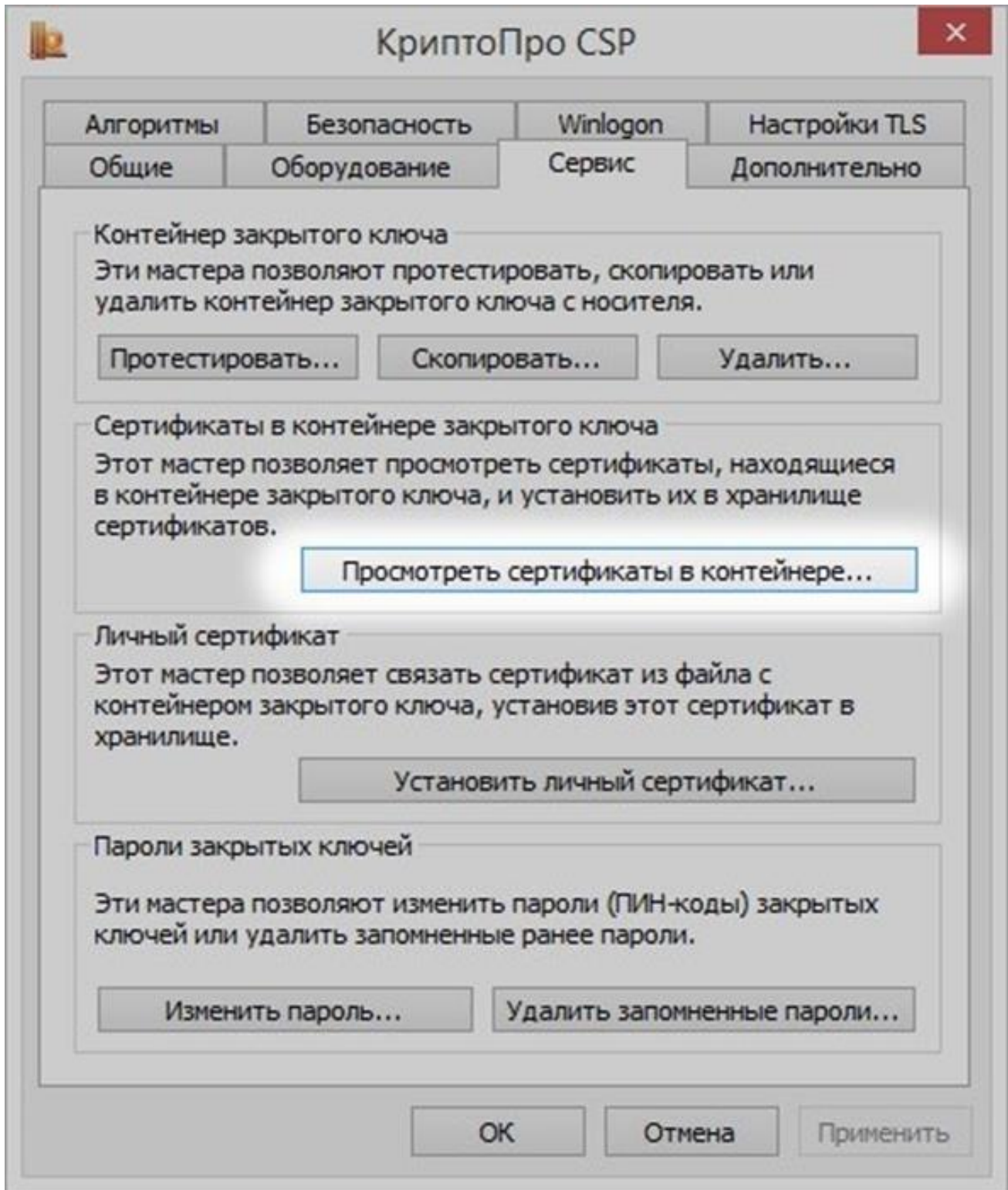
В открывшемся окошке выбираем «Обзор» и папку «Личное», далее — «Ок» и в последующем окошке выбираем «Готово».



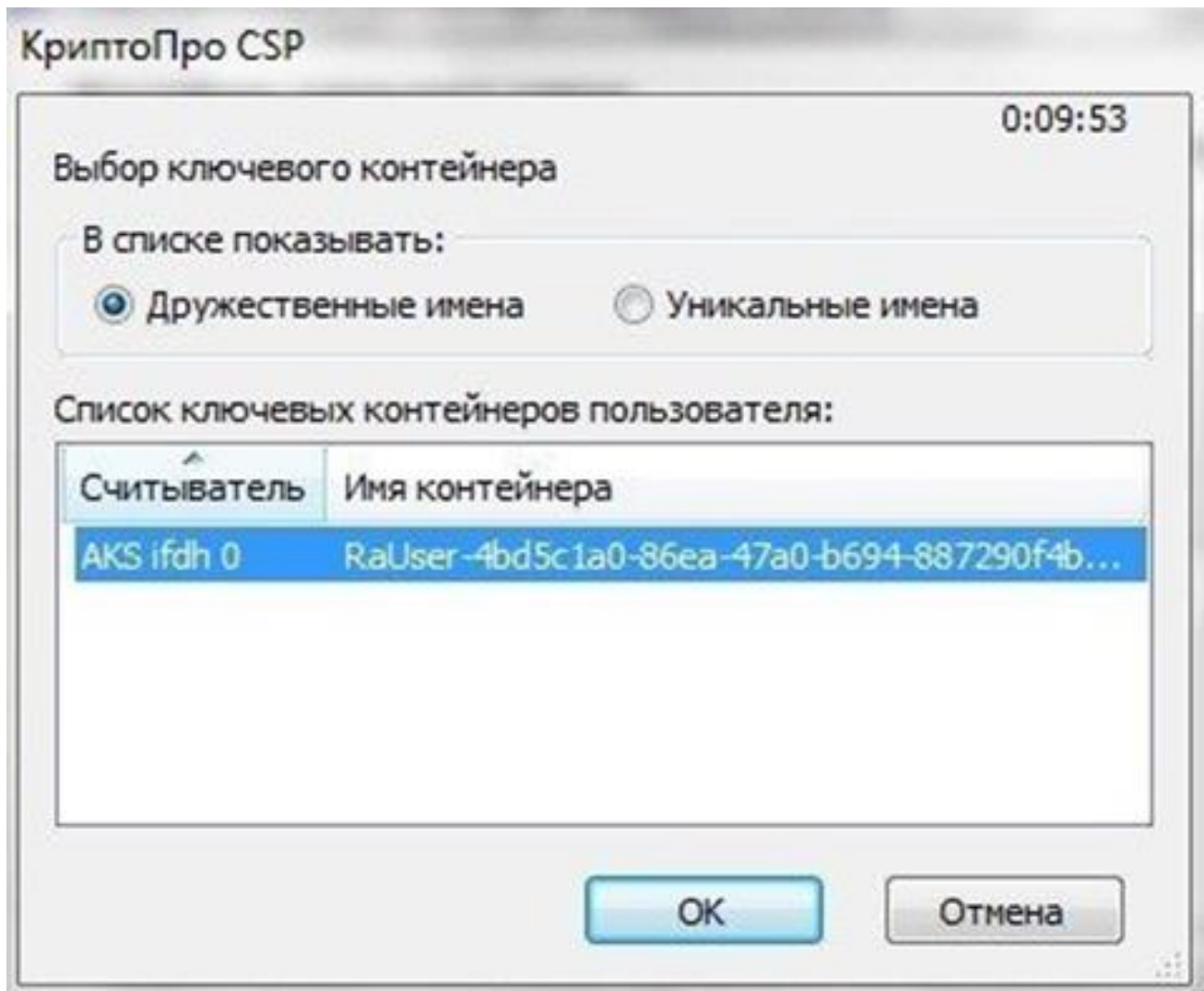
Вариант 2. Установка корневого сертификата удостоверяющего центра

Для установки сертификата вторым методом:

Запускаем программу «КриптоПро CSP», идем на закладку «Сервис» и ищем клавишу «Просмотреть сертификат в контейнере».

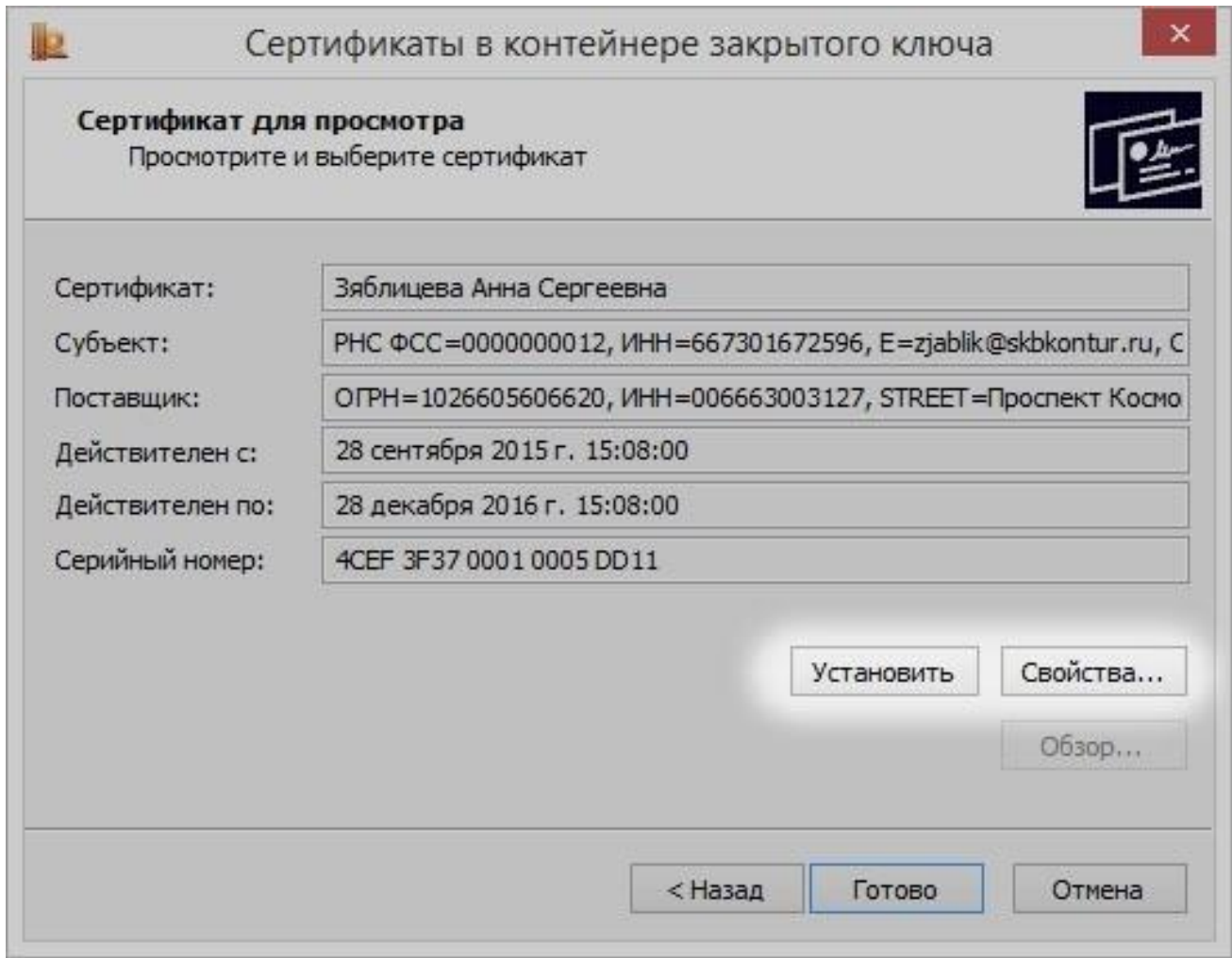


Далее — «Обзор», выбираем нужный сертификат клавишей «Ок».

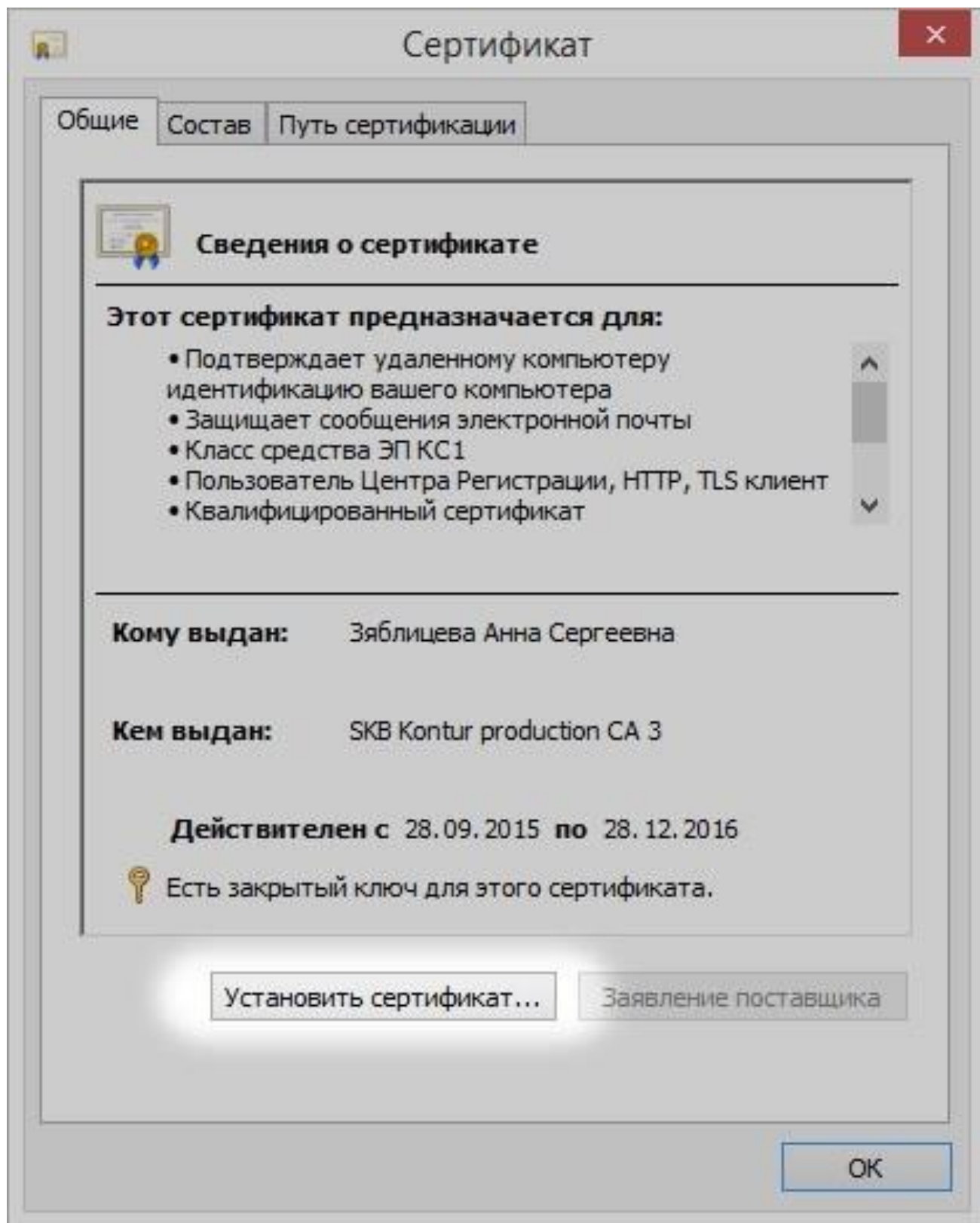


В следующем окошке выбираем «Далее», ничего не меняя.

Далее - клавишу «Свойства».



Выбираем «Установить сертификат».



Переводим переключатель в ячейку «Автоматически выбрать хранилище на основе типа сертификата» и ждем «Далее».

Раздел 6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Наряду с чтением лекций и проведением семинарских занятий неотъемлемым элементом учебного процесса является *самостоятельная работа*. При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические

способности, столь важные для успешной подготовки и защиты выпускной работы обучающегося. Формы самостоятельной работы обучающихся могут быть разнообразными. Самостоятельная работа обучающихся включает: изучение литературы, оценку, обсуждение и рецензирование публикуемых статей; ответы на контрольные вопросы; самотестирование. Выполнение всех видов самостоятельной работы увязывается с изучением конкретных тем.

Таблица 6.1

Самостоятельная работа

Наименование разделов, тем	Вопросы, выносимые на самостоятельное изучение
Тема 1. Введение в информационную безопасность	<p>Основные понятия: задачи, объект, предмет, методы информационной безопасности.</p> <p>Официальные органы, обеспечивающие информационную безопасность в Российской Федерации.</p> <p>Правовое обеспечение информационной безопасности.</p> <p>Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года.</p> <p>Составляющие концептуальной модели информационной безопасности. Понятие угроз безопасности.</p> <p>Современная концепция информационной безопасности.</p> <p>Цели защиты информации.</p> <p>Носители защищаемой информации.</p>
Тема 2. Защита от компьютерных вирусов.	<p>Способы распространения вредоносных программ. Последствия заражений вредоносной программой. Классификация вредоносных программ. Примеры угроз безопасности информации реализуемых вредоносными программами</p> <p>Ответственность за написание и распространение вредоносных программ</p> <p>Самостоятельная диагностика заражения вредоносными программами. Признаки и диагностика заражений через браузер.</p> <p>Подозрительные процессы. Сетевая активность.</p> <p>Элементы автозапуска. Основы функционирования антивирусного программного обеспечения. Технологии обнаружения вирусов.</p> <p>Классификация антивирусного программного обеспечения.</p> <p>Комплексные средства антивирусной защиты.</p>
Тема 3. Криптографическое закрытие информации	<p>Алгоритмы шифрования с симметричным и несимметричным ключами. Цифровая подпись.</p> <p>Криптографические хэш - функции. Контрольные суммы. GnuPG.</p> <p>Аутентификация пользователя. Аутентификация по паролю.</p>
Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств	<p>Предметизадачи программно-аппаратной защиты информации</p> <p>Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные при обеспечении информационной безопасности</p> <p>Архитектура системы безопасности</p> <p>Уязвимость компьютерных систем.</p> <p>Политика безопасности в компьютерных системах.</p> <p>оценка защищенности</p> <p>Механизмы защиты ...</p>
Тема 5. Защита информационно-программного обеспечения на уровне операционных систем	<p>Средства управления безопасностью.</p> <p>Система управления доступом.</p> <p>Пользователи и группы пользователей.</p> <p>Объекты. Дескриптор защиты.</p> <p>Субъекты безопасности. Процессы, потоки. Маркер доступа.</p>

Наименование разделов, тем	Вопросы, выносимые на самостоятельное изучение
и систем управления базами данных	Проверка прав доступа. Основные компоненты системы безопасности. Политика безопасности. Ролевой доступ. Привилегии. Угрозы безопасности ПО. Разрушающие программные средства. Модель угроз и принципы обеспечения безопасности ПО. Элементы модели угроз эксплуатационной безопасности ПО. Основные принципы обеспечения безопасности ПО на различных стадиях его жизненного цикла. Методы и средства анализа безопасности ПО.
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Проводные и беспроводные сети. Локальные сети и их службы. Сети под управлением сервера и одноранговые. Службы Интернета. Клиент серверный принцип. IP адрес и DNS служба. Межсетевой экран. Службы ssh, sftp, www, telnet, электронная почта. SSL. Протокол https. Html язык. Программы, выполняемые на стороне клиента или на стороне сервера. Безопасность Java, JavaScript и ActiveX.

6.1. ТЕМЫ ЭССЕ¹¹

1. Предметная задача программно-аппаратной защиты информации
2. Уязвимость компьютерных систем.
3. Политика безопасности в компьютерных системах. Оценка защищенности.
4. Управление информационными потоками достоверной вычислительной базой (ДВБ).
5. Механизмы защиты ДВБ.
6. Принципы реализации политики безопасности объекта.
7. Основные критерии оценки безопасности систем
8. Основные понятия и концепции идентификации пользователей КС
9. Схемы идентификации пользователей КС.
10. Защита информации от несанкционированного доступа и система разграничения доступа к информации в КС.
11. Организация доступа к ресурсам КС Обеспечение целостности и доступности информации в КС.
12. Сравнительный анализ программных и аппаратных комплексов, рассчитанных на защиту персональных ЭВМ от несанкционированного доступа к ЭВМ, которые разграничивают доступ к информации и устройствам ПЭВМ.
13. Аппаратно-программные средства криптографической защиты информации. Полностью и частично контролируемые компьютерные системы.
14. Устройства криптографической защиты данных серии КРИПТОН.
15. Система криптографической защиты информации от НСД КРИПТОН-ВЕТО. Комплекс КРИПТОН-ЗАМОК для ограничения доступа к компьютеру.
16. КРИПТОН Система защиты конфиденциальной информации SecretDisk. Система защиты данных CryptonSigma.
17. Методы и средства ограничения доступа к компонентам ЭВМ Защита информации в ПЭВМ.
18. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания.

¹¹¹¹ Перечень тем не является исчерпывающим. Обучающийся может выбрать иную тему по согласованию с преподавателем.

19. Современные системы защиты ПЭВМ от несанкционированного доступа к информации. («Снег-1.0», «Кобра», «Страж-1.1», «Аккорд-4», «DALLASLOCK3.1», «Редут», «ДИЗ-1 », и др).
20. Защита программ от несанкционированного копирования.. Методы, затрудняющие считывание скопированной информации. Методы, препятствующие использованию скопированной информации.
21. Основные функции средств защиты от копирования. Основные методы защиты от копирования. Криптографические методы.
22. Методы противодействия динамическим способам снятия защиты программ от копирования.
23. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция иерархии ключей.
24. Распределение ключей. Распределение ключей с участием центра распределения ключей. Протокол аутентификации и распределения ключей для симметричных криптосистем
25. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей. Прямой обмен ключами между пользователями. Алгоритм открытого распределения ключей Диффи-Хеллмана. Протокол SKIP управления криптоключами.
26. Защита программных средств от исследования. Классификация средств исследования программ. Методы защиты программ от исследования.
27. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.
28. Классификация методов защиты от компьютерных вирусов.
29. Шифрование в каналах связи компьютерной сети. Канальное шифрование. Сквозное шифрование. Комбинированное шифрование.
30. Программы-шпионы. Программные закладки. Модели воздействия программных закладок на компьютеры. Перехват. Искажение. Уборка мусора. Наблюдение и компрометация. Защита от программных закладок. Защита от внедрения программных закладок. Выявление внедренной программной закладки. Удаление внедренной программной закладки

6.2. ПРИМЕРНЫЕ ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Почему необходим перевод федеральных органов власти и бюджетных учреждений на свободное программное обеспечение?
2. Что надо делать, чтобы компьютер не «болел»?
3. Почему у пользователей Linux вирусы на компьютере редкость, а у пользователей Windows они хозяева?
4. Самые известные компьютерные преступления.
5. Почему ОС МСВС мобильная система вооруженных сил России основана на GNU/Linux, и почему армия пользуется процессором Эльбрус а не процессорами интел.
6. Почему у вируса больше шансов победить чем у антивируса?
7. Почему на мобильных устройствах часто используется Android?

Раздел 7. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

В процессе освоения учебной дисциплины «Информационные технологии для перевода» для оценивания сформированности компетенций используются оценочные средства, представленные в таблице 7.1.

Таблица 7.1

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы в соотношении с оценочными средствами

Планируемые результаты, характеризующие этапы формирования компетенции	Содержание учебного материала	Примеры контрольных вопросов и заданий для оценки знаний, умений, владений	Методы и средства контроля
ОПК-2 «способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности»			
<p><i>Знать:</i> основы информационной безопасности и защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду;</p> <p><i>Уметь:</i> реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем;</p> <p><i>Владеть:</i> представлениями о типовых разработанных средствах защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных</p>	<p>Тема 1. Введение в информационную безопасность</p> <p>Тема 2. Защита от компьютерных вирусов.</p> <p>Тема 3. Криптографическое закрытие информации</p> <p>Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств</p>	<p>Определение информационной безопасности (ИБ).</p> <p>Определение конфиденциальности, целостности и доступности. Основные подходы к обеспечению ИБ.</p> <p>Определение «уязвимости», «угрозы», «атаки» и «эксплойта». Модели угроз и виды угроз (антропогенные, техногенные, стихийные источники угроз).</p> <p>Модель нарушителя: определение хакерства. Цели и задачи хакера. «Белые», «серые» и «чёрные» хакеры.</p> <p>Социальная инженерия: определение, задачи, примеры применения для нарушения конфиденциальности, целостности и доступности информации.</p>	<p>Эссе(темы 1-10)</p> <p>Практикум(тема 1, задания 1-2; Тема 2, задание 1</p> <p>Кейсы</p> <p>Задания для самостоятельной работы (1-3)</p> <p>Тесты(тестовые задания № 1-19)</p> <p>Зачет(вопросы 1-11)</p> <p>Эссе(темы 10-20)</p> <p>Практикум(Тема 3, задание 1-3; Тема 4, задание 1-2)</p> <p>Кейсы</p> <p>Задания для самостоятельной работы</p>

систем.			(3-6) Тесты(тестовые задания № 19-38) Зачет(вопросы 11-22)
ОПК-5 «способностью самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных»			
Знать: методику работы с источниками информации Уметь: самостоятельно осуществлять поиск и подбор информации Владеть: навыками оценки и анализа информации	Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит. Парольные системы аутентификации. Стойкость парольных систем аутентификации. Взаимная проверка подлинности пользователей информационной системы. Биометрические системы аутентификации. Основные методы взлома биометрических систем аутентификации. Основные модели разграничения прав доступа: дискреционная, мандатная и ролевая модели доступа. Криптографическая защита информации: определение шифрования, расшифрования, дешифрования, криптографического ключа, хеширования информации. Симметричное и асимметричное шифрование. Примеры симметричного и асимметричного шифрования: шифр Виженера, алгоритм RSA. Электронно-цифровая подпись (ЭЦП): определение ЭЦП, схема ЭЦП, определение сертификата открытого ключа, удостоверяющего центра. Инфраструктура открытых ключей (PKI). Кодирование информации как средство обеспечения	Эссе(темы 20-30) Практикум(Тема 5, задание 1) Кейсы Задания для самостоятельной работы (5-7) Тесты(тестовые задания № 38-57) Зачет(вопросы 22-35) лабораторное занятие (1-6)

		целостности информации. Примеры алгоритмов кодирования. Стеганография как один из способов обеспечения конфиденциальности и целостности информации.	
--	--	---	--

7.2. ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЕТ)

1. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ.
2. Модели, стратегии и системы обеспечения информационной безопасности.
3. Предотвращение несанкционированного доступа к компьютерным ресурсам.
4. Основные этапы допуска к ресурсам вычислительной системы.
5. Взаимная проверка подлинности и другие случаи опознавания..
6. Произвольное и принудительное управление доступом.
7. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности.
8. Схемы заражения файлов вирусом.
9. Классификация компьютерных вирусов.
10. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов.
11. Защита от деструктивных действий и размножения вирусов.
12. Технология гарантированного восстановления вычислительной системы после заражения компьютерными вирусами.
13. Типы криптографических систем.
14. Стандарты шифрования
15. Протоколы распределения ключей.
16. Уничтожение остаточных данных.
17. Основные способы защиты от потери информации
18. Методы сжатия информации. Архивация файловых данных
19. Способы резервирования информации.
20. Технология восстановления дисковой и оперативной памяти.
21. Защита информационно-программного обеспечения на уровне операционных систем
22. Ядро безопасности ОС.
23. Аппаратная основа реализации защиты на уровне ОС.
24. Безопасные файловые системы современных ОС
25. Основные требования к подсистеме безопасности СУБД.
26. Определение полномочий пользователей по доступу к базе данных
27. Использование матрицы полномочий для разграничения доступа к элементам баз данных.
28. Мандатная система разграничения доступа.
29. Транзакция и ее свойства.
30. Инструментальные средства СУБД по обеспечению целостности баз данных.
31. Особенности применения симметрических и асимметрических систем шифрования.
32. Выработка секретных ключей по Диффи-Хеллману
33. Формирование и проверка цифровой подписи.
34. Типы межсетевых экранов, их достоинства и недостатки.
35. Ограничение доступа из локальной сети в Internet с помощью прокси-серверов.

7.3 Примерные тестовые задания для контроля (мониторинга) качества усвоения материала в т.ч. в рамках рубежного контроля знаний¹²

Выберите вариант/варианты правильного ответа:

1. В каком правовом документе дается определение термина «информационная безопасность»?

- а) Федеральный закон «Обезопасности».
- б) Стратегия национальной безопасности Российской Федерации до 2020 года.
- в) Доктрина информационной безопасности Российской Федерации.
- г) Конституция.
- д) Федеральный закон «Об информации, информационных технологиях и о защите информации».

2. Основными аспектами деятельности (задачами) информационной безопасности выступают –

- а) Конфиденциальность.
- б) Доступность.
- в) Системность.
- г) Целостность.
- д) Защита информации.

3. Постройте соответствие между методами защиты информации (левая колонка) и их характеристиками (правая колонка):

1. Правовые методы	А. Подбор сотрудников компании, а также обеспечение того, чтобы непроверенные лица не допускались к охраняемой информации
2. Программный метод	В. Разработка нормативных актов, подразумевающих административную и уголовную ответственность за хищение информации, нарушение авторских прав программистов и киберпреступления
3. Программно-аппаратный метод	С. Использование антивирусных программ пассивной защиты (брандмауэр, файрволит.п.)
4. Физические методы	Д. Изготовление аппаратных средств защиты информации, например, сетевых адаптеров в память которого встроена антивирусная программа
5. Организационные методы	Е. Включает всебя защиту кабельных систем, использование всевозможных источников бесперебойного питания, защиту помещений от постороннего доступа, резервное копирование информации
6. Административные методы	Ф. Формирование политики информационной безопасности компании

4. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:

- а) Информация
- б) Информационные технологии
- с) Информационная система
- д) Информационно-телекоммуникационная сеть
- е) Владелец информации

¹² Рубежный контроль знаний проводится для обучающихся очной формы обучения и оценивается по шкале «зачтено» \ «не зачтено»

5. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:

- a) Источник информации
- b) Потребитель информации
- c) Уничтожитель информации
- d) Носитель информации
- e) Владелец информации

6. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:

- a) База данных
- b) Информационная технология
- c) Информационная система
- d) Информационно-телекоммуникационная сеть
- e) Медицинская информационная система

7. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее владельца это:

- a) Электронное сообщение
- b) Распространение информации
- c) Предоставление информации
- d) Конфиденциальность информации
- e) Доступ к информации

8. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:

- a) Уничтожение информации
- b) Распространение информации
- c) Предоставление информации
- d) Конфиденциальность информации
- e) Доступ к информации

9. Возможность получения информации и ее использования это:

- a) Сохранение информации
- b) Распространение информации
- c) Предоставление информации
- d) Конфиденциальность информации
- e) Доступ к информации

10. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:

- a) Электронное сообщение
- b) Информационное сообщение
- c) Текстовое сообщение
- d) Визуальное сообщение
- e) SMS-сообщение

11. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

- a) Информационная система персональных данных
- b) База данных
- c) Централизованное хранилище данных

- d) Система Статэкспресс
- e) Сервер

12. К сведениям конфиденциального характера, согласно указу президента РФ от 6 марта 1997 г., относятся:

- a) Информация о распространении программ
- b) Информация о лицензировании программного обеспечения
- c) Информация, размещаемая в газетах, Интернете
- d) Персональные данные
- e) Личная тайна

13. Отношения, связанные с обработкой персональных данных, регулируются законом...

- a) «Об информации, информационных технологиях»
- b) «О защите информации»
- c) Федеральным законом «О персональных данных»
- d) Федеральным законом «О конфиденциальной информации»
- e) «Об утверждении перечня сведений конфиденциального характера»

14. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т.д. это:

- a) «Исправление персональных данных»
- b) «Работа с персональными данными»
- c) «Преобразование персональных данных»
- d) «Обработка персональных данных»
- e) «Изменение персональных данных»

15. Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных:

- a) Выделение персональных данных
- b) Обеспечение безопасности персональных данных
- c) Деаутентификация
- d) Деавторизация
- e) Деперсонификация

16. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на:

- a) Многопользовательские
- b) Однопользовательские
- c) Без разграничения прав доступа
- d) С разграничением прав доступа
- e) Системы, не имеющие подключений

17. 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:

- a) Авторизация
- b) Аутентификация
- c) Обезличивание
- d) Деперсонализация
- e) Идентификация

18. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

- a) Авторизация
- b) Обезличивание
- c) Деперсонализация
- d) Аутентификация
- e) Идентификация

19. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом

- a) Авторизация
- b) Идентификация
- c) Аутентификация
- d) Обезличивание
- e) Деперсонализация

20. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

- a) Токен
- b) Password
- c) Пароль
- d) Login
- e) Смарт-карта

21. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

- a) Идентификация
- b) Аутентификация
- c) Авторизация
- d) Экспертиза
- e) Шифрование

22. Для безопасной передачи данных по каналам интернет используется технология:

- a) WWW
- b) DICOM
- c) VPN
- d) FTP
- e) XML

23. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

- a) Антивирус
- b) Замок
- c) Брандмауэр
- d) Криптография
- e) Экспертная система

24. За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:

- a) Дисциплинарные взыскания
- b) Административный штраф
- c) Уголовная ответственность
- d) Лишение свободы

- е) Смертная казнь

25. Несанкционированный доступ к информации это:

- а) Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
- б) Работа на чужом компьютере без разрешения его владельца
- в) Вход на компьютер с использованием данных другого пользователя
- г) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
- е) Доступ к СУБД под запрещенным именем пользователя

26. «Персональные данные» это:

- а) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
- б) Фамилия, имя, отчество физического лица
- в) Год, месяц, дата и место рождения, адрес физического лица
- г) Адрес проживания физического лица
- е) Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

27. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:

- а) Выход в Интернет без разрешения администратора
- б) При установке компьютерных игр
- в) В случаях установки нелегального ПО
- г) В случае не выхода из информационной системы
- е) В любом случае неправомерного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

28. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:

- а) Нет, только к административной ответственности
- б) Нет, если это государственное предприятие
- в) Да
- г) Да, но только в случае, если действия сотрудника нанесли непоправимый вред
- е) Да, но только в случае осознанных неправомерных действий сотрудника

29. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:

- а) Идентификация
- б) Аутентификация
- в) Стратификация
- г) Регистрация
- е) Авторизация

30. Наиболее опасным источником угроз информационной безопасности предприятия являются:

- а) Другие предприятия (конкуренты)
- б) Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
- в) Рядовые сотрудники предприятия
- г) Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
- е) Хакеры

31. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru:

- a) Нет, не при каких обстоятельствах
- b) Нет, но для отправки срочных и особо важных писем можно
- c) Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
- d) Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
- e) Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

32. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:

- a) Информация составляющая государственную тайну
- b) Информация составляющая коммерческую тайну
- c) Персональная
- d) Конфиденциальная информация
- e) Документированная информация

33. Для того чтобы снизить вероятность утраты информации необходимо:

- a) Регулярно производить антивирусную проверку компьютера
- b) Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
- c) Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
- d) Защитить вход на компьютер к данным паролем
- e) Проводить периодическое обслуживание ПК

34. Пароль пользователя должен

- a) Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
- b) Содержать только цифры
- c) Содержать только буквы
- d) Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
- e) Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

35. Информационная безопасность обеспечивает...

- a) Блокирование информации
- b) Искажение информации
- c) Сохранность информации
- d) Утрату информации
- e) Подделку информации

36. Закон Российской Федерации «О государственной тайне» был принят в следующем году:

- a) 1982
- b) 1985
- c) 1988
- d) 1993
- e) 2005

37. Документированной информацией, доступ к которой ограничен в соответствии с законодательством РФ, называется

- a) Конфиденциальная
- b) Персональная

- c) Документированная
- d) Информация составляющая государственную тайну
- e) Информация составляющая коммерческую тайну

38. *Информация об уголовной ответственности за преступление в сфере компьютерной информации описана в:*

- a) 1 главе Уголовного кодекса
- b) 5 главе Уголовного кодекса
- c) 28 главе Уголовного кодекса
- d) 100 главе Уголовного кодекса
- e) 1000 главе Уголовного кодекса

39. *В статье 272 уголовного кодекса говорится...*

- a) О неправомерном доступе к компьютерной информации
- b) О создании, исполнении и распространении вредоносных программ для ЭВМ
- c) О нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети
- d) О преступлениях в сфере компьютерной информации
- e) Об ответственности за преступления в сфере компьютерной информации

40. *Федеральный закон «Об информации, информатизации и защите информации» направлен на:*

- a) Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
- b) Регулирование взаимоотношений в гражданском обществе РФ
- c) Регулирование требований к работникам служб, работающих с информацией
- d) Формирование необходимых норм и правил работы с информацией
- e) Формирование необходимых норм и правил, связанных с защитой детей от информации

41. *Хищение информации – это...*

- a) Несанкционированное копирование информации
- b) Утрата информации
- c) Блокирование информации
- d) Искажение информации
- e) Продажа информации

42. *Владельцем информации первой категории является...*

- a) Государство
- b) Коммерческая организация
- c) Муниципальное учреждение
- d) Любой гражданин
- e) Группа лиц, имеющих общее дело

43. *Владельцем информации второй категории является...*

- a) Простые люди
- b) Государство
- c) Коммерческая организация
- d) Муниципальное учреждение
- e) Некоммерческая организация

44. *Владельцем информации третьей категории является...*

- a) Люди
- b) Государство
- c) Муниципальное учреждение

- d) Учреждение
- e) Некоммерческая организация

45. Информацией, составляющей государственную тайну, владеют:

- a) Государство
- b) Только образовательные учреждения
- c) Только президиум Верховного Совета РФ
- d) Граждане Российской Федерации
- e) Только министерство здравоохранения

46. Информацией, составляющей коммерческую тайну, владеют:

- a) Государство
- b) Различные учреждения
- c) Государственная Дума
- d) Граждане Российской Федерации
- e) Медико-социальные организации

47. Персональными данными владеют:

- a) Государство
- b) Различные учреждения
- a) Государственная Дума
- b) Жители Российской Федерации
- c) Медико-социальные организации

48. Доступ к информации – это:

- a) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
- b) Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
- c) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
- d) Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
- e) Возможность получения информации и ее использования

49. Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации это:

- a) Конфиденциальная информация
- b) Документы офера и договоров
- c) Факс
- d) Личный дневник
- e) Законы РФ

50. Пластиковая карточка, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации:

- a) Токен
- b) Password
- c) Пароль
- d) Login
- e) Смарт-карта

51. Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подсоединяемые к компьютеру и имеющие собственный источник питания:

- a) Токен
- b) Автономный токен
- c) USB-токен
- d) Устройство iButton
- e) Смарт-карта

52. Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после:

- a) Включения компьютера
- b) Идентификации по логину и паролю
- c) Запроса паспортных данных
- d) Запроса доменного имени
- e) Запроса ФИО

53. Аппаратные модули доверенной загрузки «Аккорд - АМДЗ» представляют собой...

- a) Аппаратный контролер
- b) Электронный замок
- c) Система контроля
- d) Сетевой адаптер
- e) Копировальный аппарат

54. Электронные замки «Соболь» предназначены для ...

- a) Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
- b) Сканирования отпечатков пальцев
- c) Проверки скорости и загрузки файлов
- d) Общего контроля
- e) Идентификации пользователя

55. Для защиты от злоумышленников необходимо использовать:

- a) Системное программное обеспечение
- b) Прикладное программное обеспечение
- c) Антивирусные программы
- d) Компьютерные игры
- e) Музыка, видеофильмы

56. Федеральный закон "Об информации, информатизации и защите информации" дает определение информации:

- a) Текст книги или письма
- b) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- c) Сведения о явлениях и процессах
- d) Факты и идеи в формализованном виде
- e) Шифрованный текст, текст на неизвестном языке

57. Обеспечение информационной безопасности есть обеспечение...

- a) Независимости информации
- b) Изменения информации
- c) Копирования информации
- d) Сохранности информации
- e) Преобразования информации

7.4. Описание показателей и критериев оценивания сформированности компетенций на различных этапах их формирования; шкалы и процедуры оценивания

7.4.1. Вопросы и заданий для текущей и промежуточной аттестации

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Таблица 7.4.1.2

Шкала оценивания на зачете, рубежном контроле

Оценка	Критерии выставления оценки
Зачтено	Обучающийся должен: <ul style="list-style-type: none">- продемонстрировать общее знание изучаемого материала;- показать общее владение понятийным аппаратом дисциплины;- уметь строить ответ в соответствии со структурой излагаемого вопроса;- знать основную рекомендуемую программой учебную литературу.
Не зачтено	Обучающийся демонстрирует: <ul style="list-style-type: none">- незнание значительной части программного материала;- не владение понятийным аппаратом дисциплины;- существенные ошибки при изложении учебного материала;- неумение строить ответ в соответствии со структурой излагаемого вопроса;- неумение делать выводы по излагаемому материалу.

7.4.2. Письменной работы (эссе)

При оценке учитывается:

1. Правильность оформления
2. Уровень сформированности компетенций.
3. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
4. Уровень знания фактического материала в объеме программы.
5. Логика, структура и грамотность изложения письменной работы.
6. Полнота изложения материала (раскрытие всех вопросов)
7. Использование необходимых источников.
8. Умение связать теорию с практикой.
9. Умение делать обобщения, выводы.

Таблица 7.4.2.2

Шкала оценивания эссе

Оценка	Критерии выставления оценки
Зачтено	Обучающийся должен: <ul style="list-style-type: none">- продемонстрировать общее знание изучаемого материала;- показать общее владение понятийным аппаратом

	дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
Не зачтено	Обучающийся демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу

7.4.3. Тестирование

Таблица 7.4.3

Шкала оценивания

Оценка	Критерии выставления оценки
Отлично	Количество верных ответов в интервале: 71-100%
Хорошо	Количество верных ответов в интервале: 56-70%
Удовлетворительно	Количество верных ответов в интервале: 41-55%
Неудовлетворительно	Количество верных ответов в интервале: 0-40%
Зачтено	Количество верных ответов в интервале: 41-100%
Не зачтено	Количество верных ответов в интервале: 0-40%

7.5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ.

Качество знаний характеризуется способностью обучающегося точно, структурированно и уместно воспроизводить информацию, полученную в процессе освоения дисциплины, в том виде, в котором она была изложена в учебном издании или преподавателем.

Умения, как правило, формируются на занятиях семинарского типа занятиях, а также при выполнении лабораторных работ. Задания, направленные на оценку умений, в значительной степени требуют от обучающегося проявления стереотипности мышления, т.е. способности выполнить работу по образцам, с которыми он работал в процессе обучения. Преподаватель же оценивает своевременность и правильность выполнения задания.

Навыки - это умения, развитые и закрепленные осознанным самостоятельным трудом. Навыки формируются при самостоятельном выполнении обучающимися практико-ориентированных заданий, моделирующих решение им производственных и социокультурных задач в соответствующей области профессиональной деятельности, как правило, при выполнении домашних заданий, курсовых проектов (работ), научно-исследовательских работ, прохождении практик, при работе индивидуально или в составе группы и т.д. При этом обучающийся поставлен в условия, когда он вынужден самостоятельно (творчески) искать пути и средства для разрешения поставленных задач, самостоятельно планировать свою работу и анализировать ее результаты, принимать определенные решения в рамках своих полномочий, самостоятельно выбирать аргументацию и нести ответственность за проделанную работу, т.е. проявить владение навыками. Взаимодействие с преподавателем осуществляется периодически по завершению определенных этапов работы и проходит в виде консультаций. При оценке владения

навыками преподавателем оценивается не только правильность решения выполненного задания, но и способность (готовность) обучающегося решать подобные практико-ориентированные задания самостоятельно (в перспективе за стенами вуза) и, главным образом, способность обучающегося обосновывать и аргументировать свои решения и предложения.

Устный опрос - это процедура, организованная как специальная беседа преподавателя с группой обучающихся (фронтальный опрос) или с отдельными обучающимися (индивидуальный опрос) с целью оценки сформированности у них основных понятий и усвоения учебного материала.

Тесты являются простейшей формой контроля, направленная на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест может предоставлять возможность выбора из перечня ответов; один или несколько правильных ответов.

Лабораторные занятия - один из видов самостоятельной учебной работы обучающихся, которая проводится по заданию преподавателя с применением лабораторного оборудования. Содержание лабораторных работ связано с другими видами учебного эксперимента (демонстрационными опытами, решением экспериментальных задач) и научными наблюдениями. Одно из важных преимуществ лабораторных занятий по сравнению с другими видами аудиторной учебной работы заключается в интеграции теоретических знаний с практическими умениями и навыками обучающегося в едином процессе деятельности учебно-исследовательского характера. Выполнение лабораторных работ требует от обучающегося творческой инициативы, самостоятельности в принятии решений, глубокого знания учебного материала, предоставляет возможности стать "открывателем истины", положительно влияет на развитие познавательных интересов и способностей.

РАЗДЕЛ 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

8.1. Методические рекомендации по написанию эссе

Эссе (от французского *essai* – опыт, набросок) – жанр научно-публицистической литературы, сочетающей подчеркнуто-индивидуальную позицию автора по конкретной проблеме.

Главными особенностями, которые характеризуют эссе, являются следующие положения:

- собственная позиция обязательно должна быть аргументирована и подкреплена ссылками на источники, авторитетные точки зрения и базироваться на фундаментальной науке. Небольшой объем (4–6 страниц), с оформленным списком литературы и сносками на ее использование;
- стиль изложения – научно-исследовательский, требующий четкой, последовательной и логичной системы доказательств; может отличаться образностью, оригинальностью, афористичностью, свободным лексическим составом языка;
- исследование ограничивается четкой, лаконичной проблемой с выявлением противоречий и разрешением этих противоречий в данной работе.

8.2. Методические рекомендации по использованию кейсов

Кейс-метод (Casestudy) – метод анализа реальной ситуации, описание которой одновременно отражает не только какую-либо практическую проблему, но и актуализирует определенный комплекс знаний, который необходимо усвоить при разрешении данной проблемы. При этом сама проблема не имеет однозначных решений.

Кейс как метод оценки компетенций должен удовлетворять следующим требованиям:

- соответствовать четко поставленной цели создания;

- иметь междисциплинарный характер;
- иметь достаточный объем первичных и статистических данных;
- иметь соответствующий уровень сложности, иллюстрировать типичные ситуации, иметь актуальную проблему, позволяющую применить разнообразные методы анализа при поиске решения, иметь несколько решений.

Кейс-метод оказывает содействие развитию умения решать проблемы с учетом конкретных условий и при наличии фактической информации. Он развивает такие квалификационные характеристики, как способность к проведению анализа и диагностики проблем, умение четко формулировать и высказывать свою позицию, умение общаться, дискутировать, воспринимать и оценивать информацию, которая поступает в вербальной и невербальной форме.

8.3. Требования к компетентностно-ориентированным заданиям для демонстрации выполнения профессиональных задач

Компетентностно-ориентированное задание – это всегда практическое задание, выполнение которого нацелено на демонстрацию доказательств наличия у обучающихся общекультурных, общепрофессиональных и профессиональных компетенций, знаний, умений, необходимых для будущей профессиональной деятельности.

Компетентностно-ориентированные задания бывают разных видов:

- направленные на подготовку конкретного практико-ориентированного продукта (анализ документов, текстов, критика, разработка схем и др.);
- аналитического и диагностического характера, направленные на анализ различных аспектов и проблем;
- связанные с выполнением основных профессиональных функций (выполнение конкретных действий в рамках вида профессиональной деятельности, например формулирование целей миссии, и т. п.).

Раздел 8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература¹³

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. -ЭБС «IPRbooks». — 978-5-4488-0070-2. — Режим доступа: <http://www.iprbookshop.ru/63594.html>

Дополнительная литература¹⁴

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. -ЭБС «IPRbooks». — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. -ЭБС «IPRbooks». — 978-5-94774-821-5. — Режим доступа: <http://www.iprbookshop.ru/52209.html>

Крылов Г.О. Понятийный аппарат информационной безопасности [Электронный ресурс] : словарь / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА

¹³Из ЭБС института

¹⁴ Из ЭБС института

Нормативные источники

1. Конституция РФ.
2. Федеральный конституционный закон от 28.04.1995 № 1-ФКЗ «Об арбитражных судах в Российской Федерации».
3. Закон РФ от 05.03.1992 № 2446-1 «О безопасности».
4. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Закон от 27.12.1991 № 2124-1 «О средствах массовой информации».
7. Федеральный закон от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».
8. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
9. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
10. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
11. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
12. Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».
13. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
14. Федеральный закон от 10.01.2003 № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы».
15. Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».
16. Доктрина информационной безопасности Российской Федерации.
17. Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
18. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
19. Указ Президента РФ от 01.09.2004 № 1135 «Об утверждении Положения об Управлении информационного и документационного обеспечения Президента Российской Федерации».
20. Указ Президента РФ от 27.07.1992 № 802 «О научном и информационном обеспечении проблем инвалидности и инвалидов».
21. Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России».
22. Указ Президента РФ от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации».
23. Указ Президента РФ от 19.10.2005 № 1222 «Об основных документах, удостоверяющих личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащих электронные носители информации».
24. Постановление Правительства РФ от 22.10.2007 № 689 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

25. Постановление Правительства РФ от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (вместе с «Требованиями к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства Российской Федерации в сети Интернет»).
26. Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
27. Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе «Электронная Россия (2002 - 2010 годы)».
28. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
29. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Интернет-ресурсы, современные профессиональные базы данных, информационно-справочные и поисковые системы

ЭБС «IPRbooks» <http://www.iprbookshop.ru>

1. *security lab* | <http://www.securitylab.ru/>

Проект компании positivetechologies. помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.

2. *Threatpost* <https://threatpos>

Новостной сайт об информационной безопасности от KasperskyLab. Авторитетный источник, на который ссылаются ведущие новостные агентства, такие как TheNewYorkTimes и TheWallStreetJournal.

3. *Anti-Malware* | <https://www.anti-malware.ru/>

Информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме.

4. *Geektimes* | <https://geektimes.ru/hub/infosecurity/>

Популярный хаб сайта geektimes.ru про информационную безопасность. Десятки тысяч просмотров статей, публикации о новинках индустрии и активное обсуждение в комментариях.

5. *CNEWS* <http://safe.cnews.ru/>

Раздел новостного издания о высоких технологиях CNEWS, посвященный информационной безопасности. Публикуются новости и экспертные статьи.

6. *Блог Алексея Лукацкого* <http://lukatsky.blogspot.it/>

Алексей Лукацкий – признанный эксперт в области информационной безопасности, обладатель множества наград, автор статей, книг, курсов, участвует в экспертизе нормативно-правовых актов в сфере ИБ и защиты персональных данных.

7. *Блог Евгения Царева* <https://www.tsarev.biz/>

Блог участника судебных процессов в качестве эксперта по вопросам кибербезопасности и защиты информации. Публикуются еженедельные обзоры всего самого интересного в мире кибербезопасности, новости об изменениях в нормативно-правовых актах.

8. *Персональный сайт Алексея Комарова* | <https://zlonov.ru/>

Сайт эксперта в области информационной безопасности, информационных технологий, информационной безопасности автоматизированных промышленных систем управления технологическим процессом.

9. *Научный журнал «Вопросы кибербезопасности»* <http://cyberrus.com/>

Печатаются статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации.

10. *Журнал “Information Security”* <http://www.itsec.ru/articles2/allpubliks>

В журнале публикуются технические обозрения, тесты новых продуктов, а также описания комплексных интегрированных решений, внедренных на российских предприятиях и в государственных органах.

11. *Клуб информационной безопасности* <http://wiki.informationsecurity.club/doku.php/main>

Клуб информационной безопасности — некоммерческая организация, развивающая ИБ и решающая задачи в этой сфере. На сайте есть «База знаний», где можно найти нормативные документы, программное обеспечение, книги, ссылки на интересные ресурсы.

12. *ISO27000.RU* <http://www.iso27000.ru/>

Интернет-портал ISO27000.RU – это площадка для общения специалистов по ИБ. Есть тематический каталог ссылок на ресурсы по информационной безопасности и защите информации.

13. *Ассоциация по вопросам защиты информации BISA* <http://bis-expert.ru/>

Сообщество, созданное под эгидой Ассоциации BusinessInformationSecurity (BISA), выпускает свой журнал, проводит вебинары, а также является организатором мероприятий.

14. *Видеоканал компании CISCO*

<https://www.youtube.com/playlist?list=PLEnXkMoWG1q2ZroboDpbUjwrqB3wIcMYC>

Публикуются как видео для обычных пользователей, так и видео для профессионалов с разбором конкретных кейсов.

15. *Канал интернет-телекомпании BIS TV* | <https://www.youtube.com/channel/UCinmAF3guG-A5u81cWiVrRg>

Канал интернет-телекомпании BIS TV специализируется на информационной безопасности банков, кредитных организаций и платёжных систем.

16. *Dark Reading* <http://www.darkreading.com/>

Сообщество профессионалов, где обсуждаются кибер-угрозы, уязвимости и методы защиты от атак, а также ключевые технологии и методы, которые могут помочь защитить данные в будущем.

17. *Security Weekly* <https://securityweekly.com/>

Самое актуальное в формате подкастов, видео, live-трансляций. Еженедельные шоу от Securityweekly – это интервью с профессионалами, обсуждение последних событий в области информационной безопасности.

18. *Naked Security* <https://nakedsecurity.sophos.com/>

Авторитетный новостной сайт компании Sophos, цитируемый крупными изданиями. Освещается широкий круг вопросов: последние события в мире информационной безопасности, новые угрозы, обзор самых важных новостей недели.

19. *(IN) SECURE Magazine* <https://www.helpnetsecurity.com/insecuremag/>

(IN) SECURE Magazine выпускается с 2005 года и публикуется ежеквартально. Фокусируются на новых тенденциях, инсайтах, исследованиях и мнениях. В специальных ежегодных выпусках журнала освещаются такие крупные события RSA Conference и InfosecurityEurope.

20. *Security Bloggers Network* | <http://securitybloggersnetwork.com/>

Около 300 блогов и подкастов об информационной безопасности. Отличительная черта – более технический, практический подход к освещению актуальных вопросов ИБ и кибербезопасности.

Интернет-ресурсы

ЭБС «IPRbooks» <http://www.iprbookshop.ru>

УМО по классическому университетскому образованию России <http://www.umo.msu.ru>

Министерство образования и науки Российской Федерации <http://mon.gov.ru>

Современные профессиональные базы данных

Правотека.ру. – Б.г. – Доступ к данным: открытый. – Режим доступа :

<http://www.pravoteka.ru/>

Российская национальная библиотека. – Б.г. – Доступ к данным: Открытый. – Режим доступа : <http://www.nlr.ru/>

Информационно-справочные системы

<http://www.consultant.ru/>

<http://www.kremlin.ru/>

<https://digital.gov.ru/ru/documents/>

Поисковые системы

<http://www.sciencedirect.com>

<https://elibrary.ru/>

Комплект лицензионного программного обеспечения

2014-2015 учебный год:

1. Microsoft Open Value Subscription для решений Education Solutions № V723251. MDE (Windows 7, Microsoft Office 2010/2013 и Office Web Apps. ESET NOD32 Antivirus Business Edition) договор № ДЛ1807/01 от 18.07.2014г. Приложение №1 от 18 июля 2014

Справочная Правовая Система КонсультантПлюс – договор об информационной поддержке от 29.08.2008 (срок действия – бессрочный)

«ДИАЛОГ-М» - договор №41 от 14 мая 2015

2015-2016 учебный год

Microsoft Open Value Subscription для решений Education Solutions № V723251. MDE (Windows 7, Microsoft Office 2010/2013 и Office Web Apps. ESET NOD32 Antivirus Business Edition) договор № ДЛ1807/01 от 18.07.2014г. Приложение №2 от 03 июля 2015

Справочная Правовая Система КонсультантПлюс – договор об информационной поддержке от 26.12.2014 (срок действия – бессрочный)

2016-2017 учебный год

Microsoft Open Value Subscription для решений Education Solutions № V723251. MDE (Windows 7, Microsoft Office 2010/2013 и Office Web Apps. ESET NOD32 Antivirus Business Edition) договор № ДЛ1807/01 от 18.07.2014г. Приложение №3 от 04 августа 2016

Справочная Правовая Система КонсультантПлюс – договор об информационной поддержке от 26.12.2014 (срок действия – бессрочный)

«ДИАЛОГ-М» - договор №41 от 14 мая 2015

2017-2018 учебный год

Microsoft Open Value Subscription для решений Education Solutions № V723251. MDE (Windows 7, Microsoft Office 2010/2013 и Office Web Apps. ESET NOD32 Antivirus Business Edition) договор № ДЛ1807/01 от 18.07.2014г. Приложение №6 от 08 августа
 Справочная Правовая Система КонсультантПлюс – договор об информационной поддержке от 26.12.2014 (срок действия – бессрочный)
 «ДИАЛОГ-М» - договор №41 от 14 мая 2015
 2018-2019 учебный год

Microsoft Open Value Subscription для решений Education Solutions № V723251. MDE (Windows 7, Microsoft Office 2010/2013 и Office Web Apps. ESET NOD32 Antivirus Business Edition) договор № ДЛ1807/01 от 18.07.2014г. Приложение №7 от 24 июля 2018
 Справочная Правовая Система КонсультантПлюс – договор об информационной поддержке от 26.12.2014 (срок действия – бессрочный)
 «ДИАЛОГ-М» - договор №41 от 14 мая 2015

РАЗДЕЛ 10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная аудитория укомплектована специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории, включающей в себя: Комплект специальной учебной мебели. Доска аудиторная маркерная. Мультимедийное оборудование для воспроизведения аудио- и видеоматериалов в аналоговых и цифровых форматах: компьютер, проектор, экран набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации
Помещение для самостоятельной работы	компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации принтер Комплект специальной учебной мебели

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей).