Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Н. В. Ржеутская, О. А. Нистюк,
Н. И. Уласевич

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторный практикум

Рекомендовано
учебно-методическим объединением по образованию
в области информатики и радиоэлектроники
в качестве учебно-методического пособия для студентов
учреждений высшего образования по специальностям
1-40 01 01 «Программное обеспечение
информационных технологий», 1-40 05 01 «Информационные
системы и технологии (по направлениям)»,
1-98 01 03 «Программное обеспечение информационной
безопасности мобильных систем»

Минск 2024

УДК 004.056.5(076.5)
ББК 32.972.5я73
Р48

Р е ц е н з е н т ы:
кафедра естественнонаучных дисциплин и информационных технологий ГУО «Университет Национальной академии наук Беларуси» (заведующий кафедрой кандидат экономических наук, доцент *А. М. Кунявский*);
ректор УДО «Институт ИТ и бизнес-администрирования» кандидат технических наук, доцент *В. К. Дюбков*

Ржеутская, Н. В.

Р48 Основы защиты информации. Лабораторный практикум : учеб.-метод. пособие для студентов специальностей 1-40 01 01 «Программное обеспечение информационных технологий», 1-40 05 01 «Информационные системы и технологии (по направлениям)», 1-98 01 03 «Программное обеспечение информационной безопасности мобильных систем» / Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич. – Минск : БГТУ, 2024. – 124 с.

ISBN 978-985-897-133-5.

В учебно-методическом пособии рассмотрены механизмы разграничения доступа и администрирования; криптографические методы защиты информации; программные средства обеспечения безопасности передачи данных в компьютерных сетях; антивирусные средства защиты информации; технические каналы утечки информации; авторское право и патентный поиск. Представлены способы приобретения практических навыков по созданию и использованию методов и средств повышения информационной безопасности и надежности систем, основы теоретической и практической подготовки студентов в сфере интеллектуальной собственности.

УДК 004.056.5(076.5)
ББК 32.972.5я73

ISBN 978-985-897-133-5

ПРЕДИСЛОВИЕ

«Основы защиты информации» – одна из дисциплин, составляющих базу общей подготовки специалистов, в которой изучаются следующие вопросы: механизмы разграничения доступа и администрирования; криптографические методы защиты информации; программные средства обеспечения безопасности передачи данных в компьютерных сетях; антивирусные средства защиты информации; системы резервного копирования; программные средства защиты от несанкционированного копирования; создание ролей пользователей и программные средства сканирования уязвимостей информационной системы.

Для изучения предмета используются эффективные современные инновационные образовательные методики и технологии, способствующие вовлечению студентов в поиск и управление знаниями, приобретению опыта самостоятельного решения разнообразных задач.

Предлагаемое учебно-методическое пособие содержит 13 практических занятий, включающих теоретическую и практическую части по учебным темам в соответствии с утвержденной программой дисциплины. Задания для каждой практической работы содержат формулировку задачи и варианты заданий для индивидуальной самостоятельной работы студентов.

В данном учебно-методическом пособии рассматриваются следующие темы: концепция национальной безопасности Республики Беларусь; разработка средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа; политика информационной безопасности бизнес-компании; криптографическая защита информации; теория чисел; авторское право и смежные права; патентный поиск; настройка антивирусов; изучение стандартных средств для реализации симметричного и ассиметричного шифрования и др.

Практическое занятие № 1

КОНЦЕПЦИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Цель: изучить концепцию национальной безопасности Республики Беларусь.

Теоретические сведения

С развитием информационных технологий появилась необходимость стандартизации требований в области защиты информации.

Главная задача стандартов информационной безопасности – создать основу для взаимодействия между производителями, потребителями и специалистам по сертификации.

Правовое обеспечение информационной безопасности в Республике Беларусь. К международным договорам в области информационной безопасности можно отнести следующие: Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. (для Беларуси вступило в силу 4 июня 2015 г.), постановление Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 18 ноября 2005 г. № 26-7 «О гармонизации законодательства государств – участников СНГ в области информатизации и связи», Соглашение между Правительством Республики Беларусь и Правительством Республики Казахстан о сотрудничестве в области защиты информации, Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области защиты информации и т. д.

Конституция Республики Беларусь от 15 марта 1994 г. (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.), изменения и дополнения Конституции Республики Беларусь от 15 марта 2022 г. содержат статью 34, в которой гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, политической,

экономической, культурной и международной жизни, состоянии окружающей среды; указывается, что пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав.

Кодифицированные нормативные правовые акты. *Гражданский кодекс Республики Беларусь* содержит нормы, касающиеся служебной и коммерческой тайны, закрепляет такие формы отношений, как информационные услуги, электронную подпись признает как средство, подтверждающее подлинность сторон в сделках, предусматривает ответственность за незаконное использование информации (статья 140, часть 2 статьи 161, статья 1011 и др.).

Кодекс Республики Беларусь об административных правонарушениях определяет административно-правовые санкции за правонарушения в информационной сфере. К таким правонарушениям относятся: отказ в предоставлении гражданину информации, посредственно затрагивающей его права, свободы и законные интересы (статья 9.6), несанкционированный доступ к компьютерной информации (статья 22.6), нарушение правил защиты информации (статья 22.7) и др.

Уголовный кодекс Республики Беларусь закрепляет ответственность за преступления против информационной безопасности (глава 31), а также иные составы преступлений в информационной сфере (хищение путем использования компьютерной техники (статья 212), умышленное разглашение государственной тайны (статья 373), разглашение государственной тайны по неосторожности (статья 374), умышленное разглашение служебной тайны (статья 375) и др.

Трудовой кодекс Республики Беларусь для работников устанавливает обязанность хранить государственную и служебную тайну, не разглашать коммерческую тайну нанимателя, коммерческую тайну третьих лиц, к которой наниматель получил доступ (пункт 10 части 1 статьи 53).

Налоговый кодекс Республики Беларусь (общая часть) включает нормы, определяющие порядок защиты различных видов конфиденциальной информации.

Законы Республики Беларусь, в которых прописаны пункты о защите информации:

– Закон Республики Беларусь от 21 июня 2008 г. № 418-З «О регистре населения»;

– Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

– Закон Республики Беларусь от 13 июля 2006 г. № 144-З «О переписи населения»;

– Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

– указы Президента Республики Беларусь и постановления Совета Министров Республики Беларусь.

Среди данных правовых актов можно выделить основные блоки нормативных правовых актов:

– о защите информации;

– о доступе граждан к информации;

– о компетенции органов государственной власти в сфере защиты информации;

– о международном сотрудничестве в данной сфере, включая государства – члены Содружества Независимых Государств.

К таким законодательным актам можно отнести: указы Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь», от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь», от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»; постановления Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645 «О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192», от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь “Информационные технологии. Средства защиты информации. Информационная безопасность”» (ТР 2013/027/BY).

Приказы и постановления, в которых отражаются вопросы информационной безопасности. Среди приказов и постановлений Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) особое внимание заслуживают: постановление ОАЦ и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 6/8 «Об утверждении положения о порядке

ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет», приказ ОАЦ от 2 августа 2010 г. № 60 «Об утверждении Положения о порядке определения поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты», приказ ОАЦ от 16 ноября 2010 г. № 82 «Об утверждении Инструкции о порядке согласования выполнения работ и (или) оказания услуг в государственных организациях при осуществлении деятельности по технической и (или) криптографической защите информации», приказ ОАЦ от 17 декабря 2010 г. № 92 «Об утверждении перечня поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты» и др.

Государственные программы, утвержденные с целью формирования современных подходов к проектированию и созданию защищенных компьютерных систем, новых технологий и средств технической защиты информации: государственная программа развития цифровой экономики и информационного общества на 2016–2020 гг., утвержденная постановлением Совета Министров Республики Беларусь от 23 марта 2016 г. № 235; государственная научно-техническая программа «Развитие методов и средств системы комплексной защиты информации и специальных технических средств (ГНТП «Защита информации – 3») на 2016–2020 гг., утвержденная приказом Государственного комитета по науке и технологиям Республики Беларусь от 30 мая 2016 г. № 93. Основными целями последней программы являются:

– совершенствование нормативно-методической базы в области защиты информации;

– разработка и совершенствование высокопроизводительных средств защиты информации, средств оценки степени защищенности информационных систем, специальных технических средств;

– создание научно-технических условий для эффективного обеспечения безопасности информации на критически важных объектах информатизации и повышения степени защищенности объектов информатизации, систем связи и передачи данных;

– обеспечение импортозамещения средств защиты информации и специальных технических средств.

В Республике Беларусь существует необходимость принятия Концепции информационной безопасности, которая бы комплексно урегулировала данную сферу отношений и отразила государственную политику в сфере обеспечения информационной безопасности, меры защиты информации, виды и источники угроз в сфере информационной безопасности, первоочередные мероприятия по обеспечению информационной безопасности. Концепция информационной безопасности Республики Беларусь должна развивать и дополнять Конституцию Республики Беларусь и Концепцию национальной безопасности Республики Беларусь.

Контрольные вопросы

1. Что такое информационная безопасность?
2. Перечислите основные национальные интересы в информационной сфере.
3. Какие основные угрозы национальной безопасности, связанные с ИТ-сферой, вы знаете?
4. Назовите основные внутренние и внешние источники угроз национальной безопасности в информационной сфере.
5. Перечислите основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере.

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе.
2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).
3. Ответы на вопросы.
4. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

Изучите **Концепцию национальной безопасности Республики Беларусь,** утвержденную Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575.

Практическое занятие № 2

РЕШЕНИЕ ЗАДАЧИ РАЗРАБОТКИ СРЕДСТВ ЗАЩИТЫ ДЛЯ ОБЕСПЕЧЕНИЯ МАКСИМАЛЬНОЙ ЭФФЕКТИВНОСТИ ОБЪЕКТА В УСЛОВИЯХ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Цель: научиться решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

Теоретические сведения

Все методы защиты информации по характеру проводимых действий можно разделить на следующие:

– законодательные (правовые);

– организационные;

– технические;

– комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью

технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е. комплексно.

Принципиальным вопросом при определении уровня защищенности объекта является выбор критериев. Рассмотрим один из них – широко известный критерий «эффективность – стоимость».

Пусть имеется информационный объект, который при нормальном (идеальном) функционировании создает положительный эффект (экономический, политический, технический и т. д.). Этот эффект обозначим через E_0. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т. д.) на величину ΔE. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

$$E = E_0 - \Delta E. \tag{1}$$

Относительная эффективность:

$$\delta = \frac{E}{E_0} = \frac{E - \Delta E}{E_0} = 1 - \frac{\Delta E}{E_0}. \tag{2}$$

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от ΔE:

$$U = f(\Delta E). \tag{3}$$

Будем считать, что установка на объект средств защиты информации уменьшает негативное действие несанкционированного доступа на эффективность функционирования объекта. Обозначим снижение эффективности функционирования объекта при наличии средств защиты через $\Delta E_з$, а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект – через K, тогда

$$\Delta E_з = \frac{\Delta E}{K}, \tag{4}$$

где $K \geq 1$.

Выражения (1), (2) примут вид:

$$E_з = E_0 - \Delta E_з = E_0 - \frac{\Delta E}{K}; \tag{5}$$

$$\delta_з = \frac{E_з}{E_0} = \frac{E_0 - \Delta E_з}{E_0} = 1 - \frac{\Delta E}{E_0} = 1 - \frac{\Delta E}{KE_0}. \tag{6}$$

Стоимость средств защиты зависит от их эффективности, и в общем случае K – это возрастающая функция от стоимости средств защиты (C):

$$K = f(C). \tag{7}$$

Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту составит:

$$U_\Sigma = \frac{U}{K} + C = \frac{U}{f(C)} + C. \tag{8}$$

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т. д.), то U_Σ непосредственно изменяет эффективность:

$$E_з = E_0 - \frac{\Delta E}{K} - C. \tag{9}$$

Таким образом, классическая постановка задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

$$U_\Sigma \to \min, \quad C = C_{опт} \tag{10}$$

или

$$\left.\begin{aligned} E_з &\to \max, \quad C = C_{опт}; \\ \delta_з &\to \max, \quad C = C_{опт}. \end{aligned}\right\} \tag{11}$$

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется отсутствием зависимостей $K = f(C)$ и особенно оценки ущерба от несанкционированного доступа.

И если зависимость коэффициента защищенности от стоимости средств защиты можно получить, имея технические и стоимостные характеристики доступных средств защиты, то оценить реальный ущерб от несанкционированного доступа чрезвычайно сложно, так как этот ущерб зависит от множества трудно прогнозируемых факторов: наличия физических каналов несанкционированного доступа, квалификации злоумышленников, их интереса к объекту, последствий несанкционированного доступа и т. д.

Вместе с тем для объектов, на которые возлагаются ответственные задачи и для которых несанкционированный доступ влечет катастрофические потери эффективности их функционирования, влиянием стоимости средств защиты на эффективность можно пренебречь, т. е. если

$$C \ll U, \tag{12}$$

то

$$U_{\Sigma} = \frac{U}{f(C)}. \tag{13}$$

В этом случае выражение (11) и (12) принимают вид:

$$U_{\Sigma} \to \min, \quad C \le C_{\text{доп}} \tag{14}$$

или

$$\left.\begin{aligned} E_{\text{з}} &\to \max, \quad C \le C_{\text{доп}}; \\ \delta_{\text{з}} &\to \max, \quad C \le C_{\text{доп}}, \end{aligned}\right\} \tag{15}$$

где $C_{\text{доп}}$ – допустимые расходы на защиту.

Контрольные вопросы

1. Что такое технический канал утечки информации?
2. Чем отличаются пассивные и активные методы защиты информации от утечки по техническим каналам?
3. Приведите примеры пассивных методов защиты информации.
4. Перечислите примеры активных методов защиты информации.
5. По характеру проводимых действий как разделяются все методы защиты информации?

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания.

2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).

3. Условие задания (индивидуальный вариант задания).

4. Исполнительская часть.

5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

Решите задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом. Варианты выполнения задания соответствуют номеру студента по журналу группы.

Номер варианта	E_0	E	K	C
1	10 000	9000	5	500
2	100 000	90 000	50	5000
3	20 000	18 000	10	1000
4	15 000	12 000	2	1000
5	11 000	9500	3	1500
6	12 000	11 000	6	300
7	13 000	12 000	5	600
8	16 000	13 000	6	1000
9	17 000	15 000	7	800
10	18 000	15 000	6	900
11	19 000	17 000	4	800
12	21 000	18 000	3	900
13	22 000	17 000	10	1000
14	25 000	20 000	8	2000
15	26 000	20 000	7	3000
16	30 000	25 000	10	3000
17	20 000	19 000	5	500
18	110 000	91 000	50	5000
19	27 000	20 000	10	1000
20	25 000	12 000	2	1000
21	31 000	25 000	3	1500
22	32 000	26 000	6	3000
23	33 000	22 000	5	6000
24	26 000	23 000	6	1000
25	22 000	20 000	6	1000
26	23 000	20 000	5	1000

Практическое занятие № 3

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-КОМПАНИИ

Цель: разработать проект политики информационной безопасности бизнес-компании.

Теоретические сведения

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Политика безопасности должна включать в себя анализ возможных угроз и выбор мер противодействия.

Гарантированность – мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки общего замысла и исполнения системы в целом и ее компонентов.

Механизм подотчетности (протоколирования): надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом.

Периметр безопасности – граница надежной вычислительной базы. То, что внутри периметра, считается надежным, а то, что вне, – нет.

Согласно стандарту «Критерии определения безопасности компьютерных систем» («Оранжевая книга»), политика безопасности должна включать в себя по крайней мере следующие элементы:

– произвольное управление доступом;
– безопасность повторного использования объектов;
– метки безопасности;
– принудительное управление доступом.

Произвольное управление доступом – это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

Текущее состояние прав доступа при произвольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах – объекты. В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для субъекта по отношению к объекту: например, чтение, запись, выполнение, возможность передачи прав другим субъектам и т. п.

Безопасность повторного использования объектов – важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т. п.), для дисковых блоков и носителей в целом.

Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности «повторного использования субъектов». Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае новый сотрудник может получить ранее использовавшийся идентификатор, а с ним и все права своего предшественника.

Метки безопасности используются для реализации принудительного управления доступом к субъектам и объектам. Метка субъекта описывает его благонадежность, метка объекта – степень «закрытости» содержащейся в нем информации.

Согласно «Оранжевой книге», метки безопасности состоят из двух частей – **уровня секретности** и **списка категорий.** Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

– совершенно секретно;
– секретно;
– конфиденциально;
– несекретно.

Категории образуют неупорядоченный набор. Их назначение – описать предметную область, к которой относятся данные. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности, при этом субъект не может получить доступ к «чужим» категориям, даже если его уровень благонадежности – «совершенно секретно».

Главная проблема, касающаяся меток, – это обеспечение их целостности:

– не должно быть непомеченных субъектов и объектов;

– при любых операциях с данными метки должны оставаться правильными.

Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности.

Существует разделение устройств на многоуровневые и одноуровневые. На многоуровневых устройствах может храниться информация разного уровня секретности. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной меткой.

Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен – читать можно только то, что положено.

Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. В реальной жизни произвольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

Цель подотчетности – в каждый момент времени знать, кто работает в системе и что он делает.

Средства подотчетности делятся на три категории:

– идентификация и аутентификация;

– предоставление надежного пути;

– анализ регистрационной информации (аудит).

Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. В свою очередь система должна проверить подлинность личности пользователя, т. е. что он является именно тем, за кого себя выдает.

Идентификация и аутентификация – первый и важнейший программно-технический рубеж информационной безопасности. Если не составляет проблемы получить доступ к системе под любым именем, то другие механизмы безопасности, например управление доступом, очевидно, теряют смысл.

Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя другие, потенциально опасные, компоненты системы. Цель предоставления надежного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Относительно несложно реализовать надежный путь, если используется неинтеллектуальный терминал – достаточно иметь зарезервированную управляющую последовательность. Если же пользователь общается с интеллектуальным терминалом, персональным компьютером или рабочей станцией, задача обеспечения надежного пути становится чрезвычайно сложной, если вообще разрешимой.

Аудит имеет дело с действиями, так или иначе затрагивающими безопасность системы. К числу таких событий, например, относятся:

– вход в систему (успешный или нет);

– выход из системы;

– обращение к удаленной системе;

– операции с файлами (открыть, закрыть, переименовать, удалить);

– смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Протоколирование помогает следить за пользователями и реконструировать прошедшие события. Слежка важна в первую очередь как профилактическое средство. Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются.

Гарантированность – это мера уверенности, с которой можно утверждать, что для проведения в жизнь сформулированной политики безопасности выбран подходящий набор средств и что каждое из этих средств правильно исполняет отведенную ему роль.

В «Оранжевой книге» рассматриваются два вида гарантированности – операционная и технологическая.

Операционная гарантированность включает в себя проверку следующих элементов:

– архитектура системы;

– целостность системы;

– анализ тайных каналов передачи информации;

– надежное администрирование;

– надежное восстановление после сбоев.

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

Среди **архитектурных решений**, предусматриваемых «Оранжевой книгой», упомянем следующие:

– деление аппаратных и системных функций по уровням привилегированности и контроль обмена информацией между уровнями (принцип минимизации привилегий – каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций);

– защита различных процессов от взаимного влияния;

– наличие средств управления доступом;

– структурированность системы, явное выделение надежной вычислительной базы, обеспечение компактности этой базы.

Целостность системы в данном контексте означает, что аппаратные и программные компоненты надежной вычислительной базы работают должным образом и что имеется аппаратное и программное обеспечение для периодической проверки целостности.

Надежное администрирование в трактовке «Оранжевой книги» подразумевает, что должны быть логически выделены три роли – системного администратора, системного оператора и администратора безопасности.

Надежное восстановление после сбоев – вещь необходимая, однако ее реализация может быть сопряжена с серьезными техническими трудностями. Прежде всего должна быть сохранена целостность информации и, в частности, целостность меток безопасности. Возможна ситуация, когда сбой приходится на момент записи нового файла с совершенно секретной информацией. Если файл окажется с неправильной меткой, информация может быть скомпрометирована.

Надежное восстановление включает в себя два вида деятельности – подготовку к сбою (отказу) и собственно восстановление. Подготовка к сбою – это и регулярное выполнение резервного копирования, и выработка планов действий в экстренных случаях, и поддержание запаса резервных компонентов. Восстановление связано с перезагрузкой системы и выполнением ремонтных и/или административных процедур.

Технологическая гарантированность охватывает весь жизненный цикл системы, т. е. периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных «закладок».

Первое, на что обычно обращают внимание, это **тестирование.** Тесты должны показать, что защитные механизмы функционируют в соответствии со своим описанием и что не существует очевидных способов обхода или разрушения защиты. Должна быть уверенность, что надежную вычислительную базу нельзя привести в состояние, когда она перестанет обслуживать пользовательские запросы.

Документация – необходимое условие гарантированной надежности системы и одновременно инструмент проведения политики безопасности. Без документации люди не будут знать, какой политике следовать и что для этого нужно делать.

Согласно «Оранжевой книге», в комплект документации надежной системы должны входить следующие тома:

– руководство пользователя по средствам безопасности;

– руководство администратора по средствам безопасности;

– тестовая документация;

– описание архитектуры.

На практике требуется еще по крайней мере одна книга – письменное изложение политики безопасности данной организации.

Работы по обеспечению режима информационной безопасности:

– определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;

– оценка рисков;

– выбор контрмер, обеспечивающих режим информационной безопасности;

– управление рисками;

– аудит системы управления информационной безопасностью;

– выработка политики безопасности.

Существует несколько этапов разработки политики безопасности компании.

Этап 1. Выбор национальных и международных руководящих документов и стандартов в области информационной безопасности и формулирование на их базе основных требований и положений политики информационной безопасности компании, включая:

– управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту;

– вопросы резервного копирования;

– проведение ремонтных и восстановительных работ;

– информирование об инцидентах в области информационной безопасности и пр.

Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности компьютерных информационных систем (КИС). Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.

Этап 3. Структуризация контрмер по защите информации по следующим основным уровням: административному, процедурному, программно-техническому.

Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере информационной безопасности. Назначение периодичности проведения совещаний по тематике информационной безопасности на уровне руководства, в том числе периодического пересмотра положений политики информационной безопасности, а также порядка обучения всех категорий пользователей информационной системы в области информационной безопасности. Известно, что выработка политики безопасности организации – наименее формализованный этап. Однако в последнее время именно здесь сосредоточены усилия многих специалистов по защите информации.

Этап 5. Определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания. На этом этапе определяются границы системы, для которой должен

быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности строится именно в этих границах.

Основой мер **административного уровня,** т. е. мер, предпринимаемых руководством организации, является политика безопасности.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Определение политики информационной безопасности должно сводиться к следующим практическим шагам.

1. Определение используемых руководящих документов и стандартов в области информационной безопасности, а также основных положений политики информационной безопасности, включая:

– управление доступом к средствам вычислительной техники, программам и данным;

– антивирусную защиту;

– вопросы резервного копирования;

– проведение ремонтных и восстановительных работ;

– информирование об инцидентах в области информационной безопасности.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области информационной безопасности. Должна быть определена периодичность проведения совещаний по тематике информационной безопасности на уровне руководства, включая периодический пересмотр положений политики информационной безопасности, а также порядок обучения всех категорий пользователей информационной системы по вопросам информационной безопасности.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен

режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Описание границ системы, для которой должен быть обеспечен режим информационной безопасности, рекомендуется выполнять по следующему плану.

1. Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой или модернизацией автоматизированной системы обработки информации.

2. Размещение средств вычислительной техники и поддерживающей инфраструктуры. Модель иерархии средств вычислительной техники.

3. Ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы следующих классов: средства вычислительной техники, данные, системное и прикладное программное обеспечение. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методология оценок по этим критериям.

4. Технология обработки информации и решаемые задачи. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

В результате должен быть составлен документ, в котором:

– зафиксированы границы и структура системы;

– перечислены ресурсы, подлежащие защите;

– дана система критериев для оценки их ценности.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

В случае когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму

информационной безопасности является недостаточным. Для того чтобы сформулировать дополнительные требования, необходимо:

– определить ценность ресурсов;

– к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

– оценить вероятности угроз;

– определить уровень уязвимости ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Процесс оценивая рисков содержит несколько этапов:

1) идентификация ресурса и оценивание его количественных показателей (определение негативного воздействия);

2) оценивание угроз;

3) оценивание уязвимостей;

4) оценивание существующих и предполагаемых средств обеспечения;

5) оценивание рисков.

На основании оценивания рисков выбираются средства, обеспечивающие режим информационной безопасности. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Риск характеризует опасность, которой могут подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и

степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления информационной безопасностью.

При оценивании рисков учитывается:

– ценность ресурсов;

– оценка значимости угроз;

– эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

– количественными (например, стоимостные);

– качественными (могут быть построены на использовании таких понятий, как «умеренный» или «чрезвычайно опасный»);

– их комбинацией.

Вероятность того, что угроза реализуется, определяется следующими факторами:

– привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

– возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

– технические возможности угрозы, используемые при умышленном воздействии со стороны человека;

– вероятность того, что угроза реализуется;

– степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях.

К **процедурному уровню** относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

– управление персоналом;

– физическая защита;

– поддержание работоспособности;

– реагирование на нарушения режима безопасности;

– планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности должны существовать квалификационные требования по информационной безопасности. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Планирование восстановительных работ предполагает:

– слаженность действий персонала во время и после аварии;

– наличие заранее подготовленных резервных производственных площадок;

– официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;

– схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающей в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой **программно-технического уровня** являются следующие механизмы безопасности:

– идентификация и аутентификация пользователей;

– управление доступом;

– протоколирование и аудит;

– криптография;

– экранирование;

– обеспечение высокой доступности и т. д.

Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивыми к сетевым угрозам, учитывать специфику отдельных сервисов.

Контрольные вопросы

1. Что такое политика безопасности?
2. Что означают метки безопасности?
3. Какие работы производятся по обеспечению режима информационной безопасности?
4. Какие практические шаги осуществляются для определения политики информационной безопасности?
5. Что является основой программно-технического уровня для обеспечения безопасности?

Оформление отчета по заданию

1. Титульный лист.
2. Введение (обосновывается важность разработки политики информационной безопасности).
3. Описание структуры бизнес-компании (выбор компании предварительно согласовывается с преподавателем).
4. Оценка рисков.
5. Разработка мер защиты.
6. Выводы.

Задание для выполнения

Разработайте проект политики информационной безопасности компании, оформив результаты в виде пояснительной записки. Вариант выполнения заданий соответствует номеру студента по журналу группы.

Электронный вариант вносится в электронную тетрадь и показывается преподавателю для предварительной проверки (объем – 10–20 страниц).

После предварительной проверки пояснительная записка распечатывается и проект политики информационной безопасности бизнес-компании защищается в указанные преподавателем сроки.

Номер варианта	Тема
1	Университет
2	Колледж
3	Средняя школа
4	Больница
5	Поликлиника
6	Банк
7	Библиотека
8	Оператор мобильной связи
9	Завод
10	Типография
11	Риэлтерская компания
12	Туристическая компания
13	Маркетинговое агентство
14	Хозяйственный магазин
15	Интернет-магазин
16	Детский сад
17	Военкомат
18	Строительная организация
19	Таксопарк
20	Рекламное агентство
21	Логистическая компания
22	Фабрика
23	Автобусный парк
24	ЖЭС
25	Паспортный стол
26	Профсоюзная организация
27	Стоматология
28	Тренажерный зал
29	Дорожно-ремонтная служба
30	SPA-салон

Практическое занятие № 4

НАСТРОЙКА БРАНДМАУЭРА WINDOWS

Цель: овладеть навыками настройки и использования брандмауэра Windows.

Теоретические сведения

Брандмауэр (межсетевой экран) – это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера брандмауэр блокирует эти данные (рис. 1).

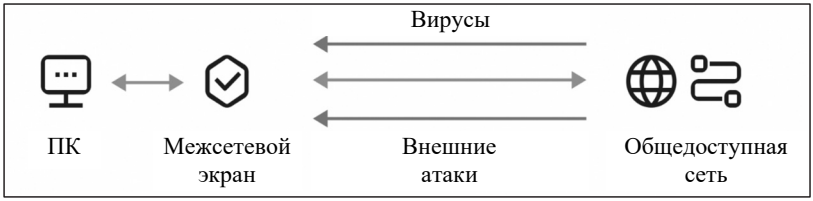

Рис. 1. Принцип действия брандмауэра

Межсетевой экран является одним из основных компонентов защиты сетей наряду с интернет-протоколом межсетевого обмена (Internet Security Protocol – IPSec). Межсетевой экран осуществляет надежную аутентификацию пользователей и защиту от несанкционированного доступа.

Отметим, что большая часть проблем с информационной безопасностью сетей связана с «прародительской» зависимостью коммуникационных решений от операционной системы UNIX – особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд интернет-служб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol – TCP/IP) имеет «бреши» в защите.

К числу таких служб и протоколов относятся:

– служба сетевых имен (Domain Name Server – DNS);

– доступ к всемирной паутине WWW;

– программа электронной почты Send Mail;

– служба эмуляции удаленного терминала Telnet;

– простой протокол передачи электронной почты (Simple Mail Transfer Protocol – SMTP);

– протокол передачи файлов (File Transfer Protocol);

– графическая оконная система X Windows.

Настройки межсетевого экрана, т. е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах – запрещать все, что не разрешено в явной форме, и разрешать все, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жестко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как предоставляет пользователям больше возможностей «обойти» межсетевой экран и использовать запрещенные сервисы через нестандартные порты (User Data Protocol – UDP), которые не запрещены политикой безопасности.

Преимущества использования брандмауэра включают защиту компьютера от несанкционированных доступов и атак, контроль трафика в сети, возможность блокировать вредоносные программы и защитить данные. Он также помогает предотвратить различные типы кибератак, обеспечивая безопасность системы в целом и сети.

Для настройки брандмауэра Windows первоначально необходимо открыть панель управления, выбрать «Система и безопасность» и затем «Брандмауэр Windows». Здесь можно управлять разрешениями для различных приложений и служб, а также создавать правила для блокировки или разрешения трафика.

Создание правила по ограничению доступа программ к сети. Для создания правила по ограничению доступа программ к сети необходимо открыть панель управления в меню «Пуск». В зависимости от версии операционной системы Windows может отображаться классический вид (рис. 2) панели управления или с разделениями по категориям (рис. 3).

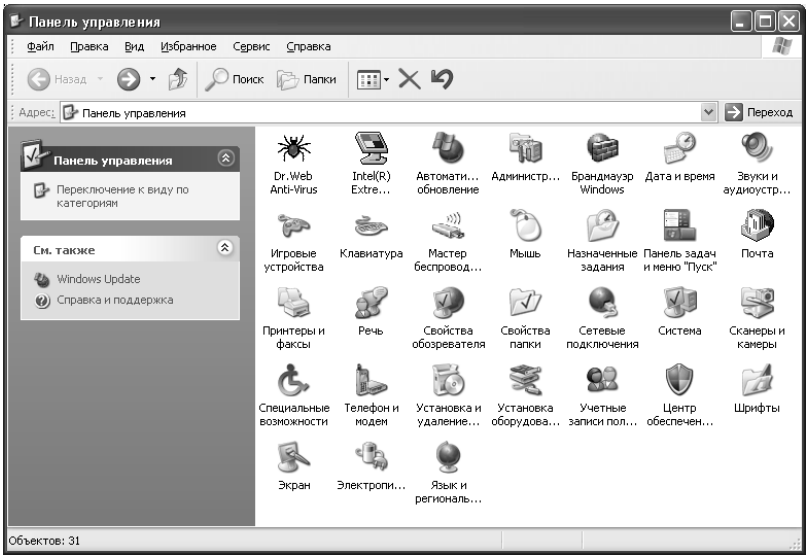

Рис. 2. Классический вид панели управления

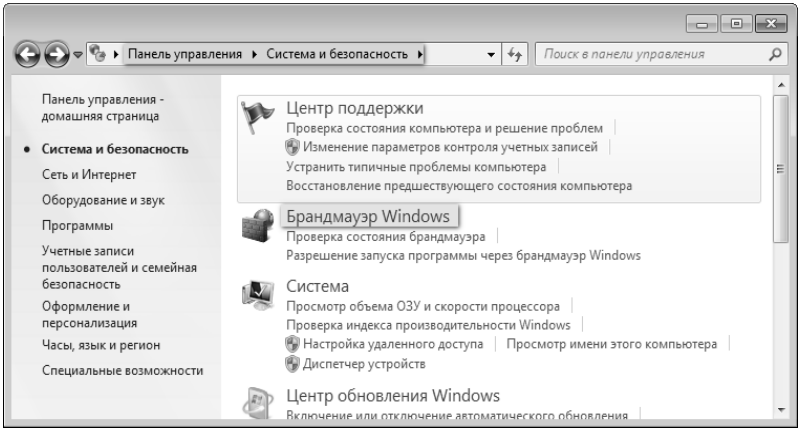

Рис. 3. Вид панели управления с разделением по категориям

На первом этапе необходимо включить брандмауэр, в случае если он был ранее выключен. Нужно выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows» (рис. 4).

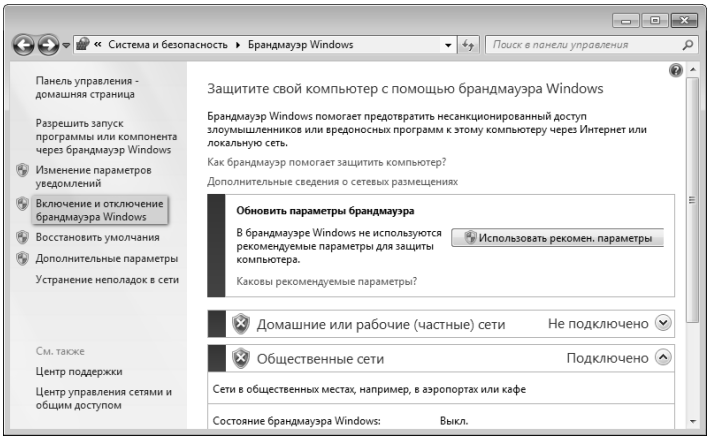

Рис. 4. Брандмауэр Windows

В появившемся окне переключаем параметры на значение «Включение брандмауэра Windows» (рис. 5).

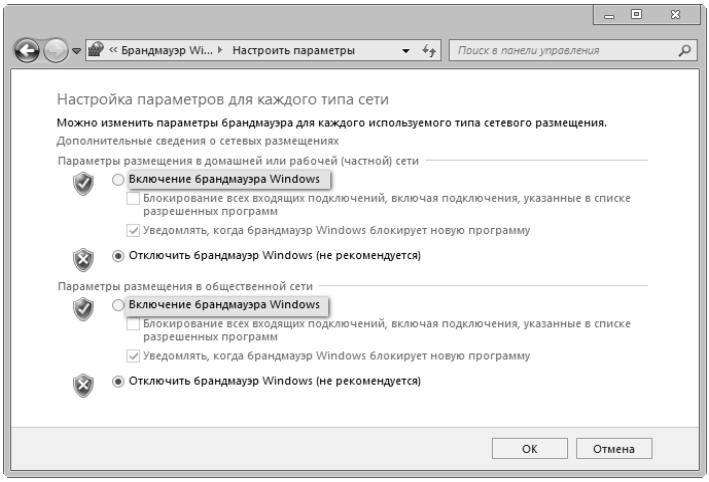

Рис. 5. Включение брандмауэра Windows

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого выбираем вкладку «Дополнительные параметры» (рис. 6).

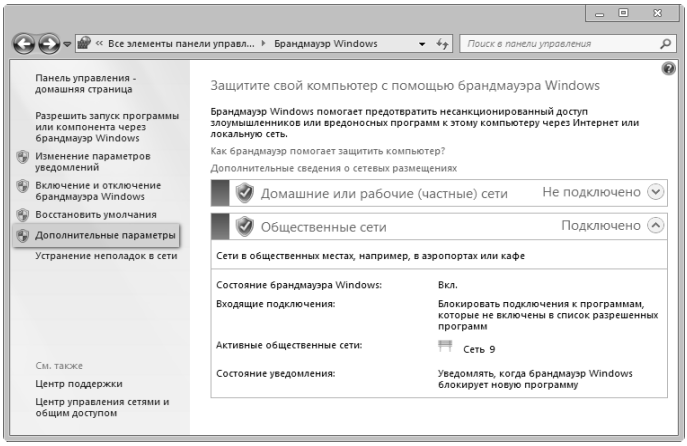

Рис. 6. Включенный брандмауэр

В открывшемся окне щелкаем мышью в левой панели по строке «Правила для входящих подключений», затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели (рис. 7).

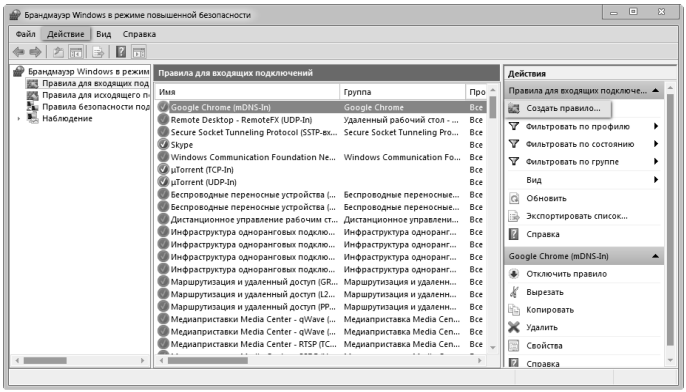

Рис. 7. Создание правила

В открывшемся мастере создания правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы) (рис. 8).

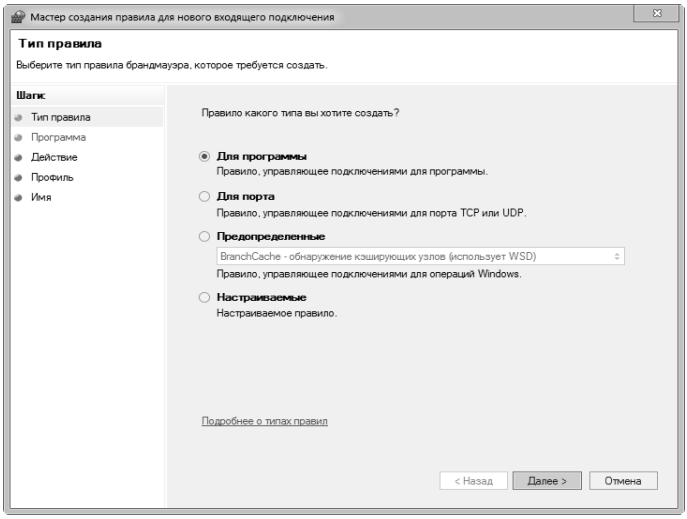

Рис. 8. Выбор типа правила

При ограничении работы программы далее необходимо указать ее путь обязательно через папку, в которой она установлена, а не через ярлыки (рис. 9).

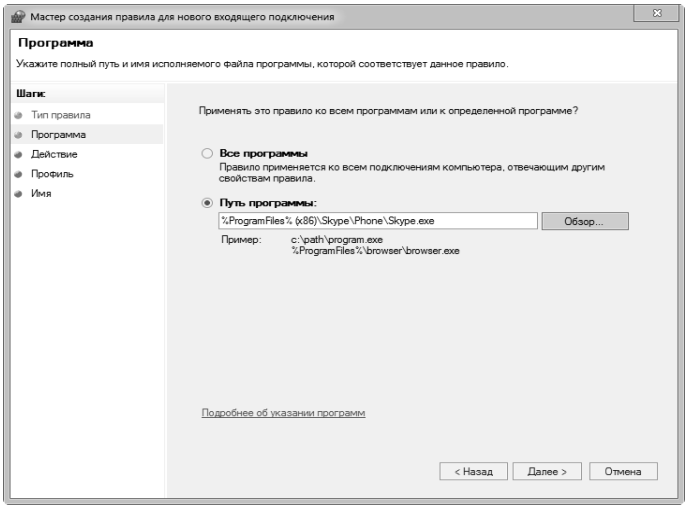

Рис. 9. Настройка пути программы

Далее указывается, какое именно действие вы хотите применить. В данном случае необходимо блокировать подключение (рис. 10).

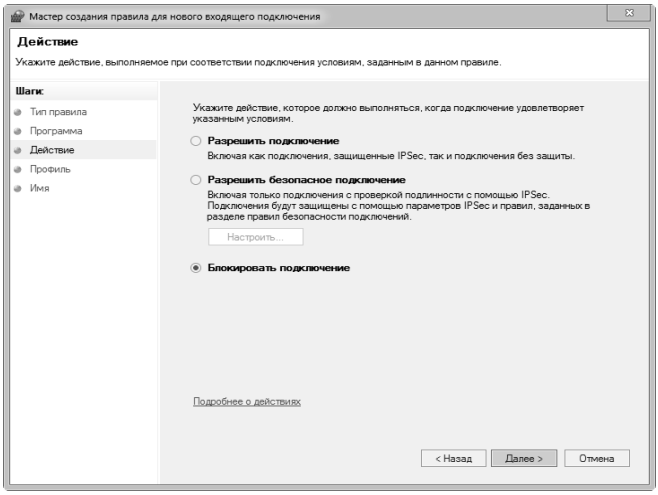

Рис. 10. Выбор действия

В следующем окне указываем имя правила (рис. 11).

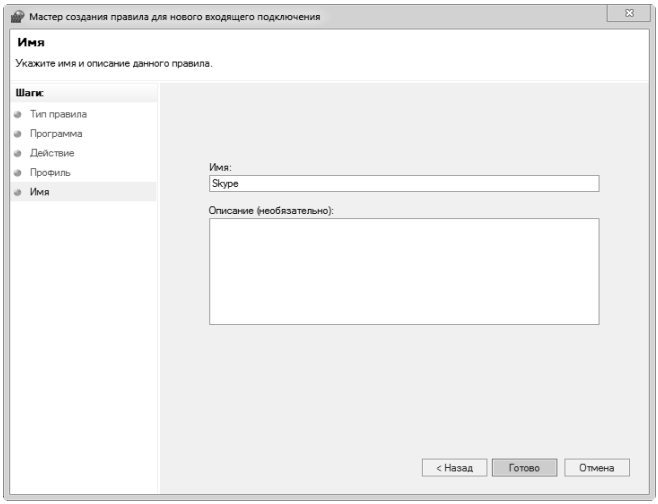

Рис. 11. Окно ввода имени

В общем списке появляется созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели (рис. 12).

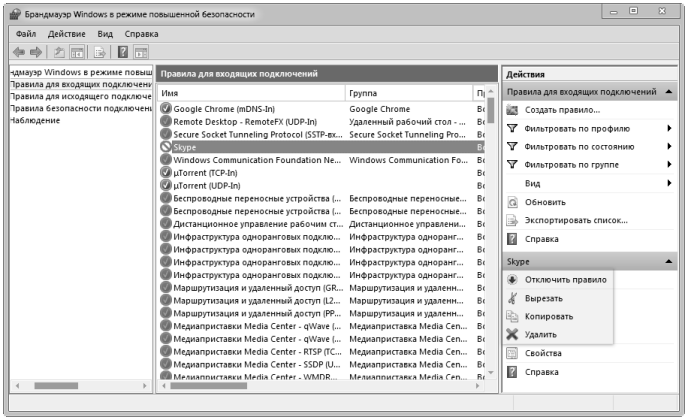

Рис. 12. Созданное правило

При двойном нажатии на правило отображаются его свойства (рис. 13).

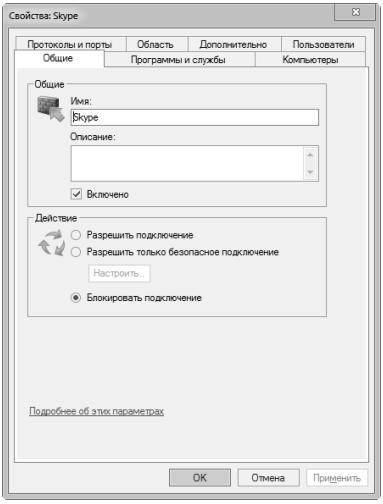

Рис. 13. Свойства правила

Аналогично создаются и правила для исходящих подключений.

Перечень команд, выполняемых через командную строку (Меню → Выполнить):

– администрирование – control admintools;
– администратор источников данных – odbccp32.cpl;
– восстановление системных файлов – sfc /scannow;
– дефрагментация дисков – dfrg.msc;
– диспетчер проверки драйверов – verifier;
– диспетчер служебных программ – utilman;
– групповая политика – gpedit.msc;
– Dr. Watson – drwtsn32;
– запросы операторов съемных озу – ntmsoprq.msc;
– защита бд учетных записей – syskey iexpress-iexpress;
– инфраструктура управления – wmimgmt.msc;
– проверка дисков – chkdsk;
– калькулятор – calc;
– командная строка – cmd;
– консоль управления – dcomcnfg;
– локальные параметры безопасности – secpol.msc;
– локальные пользователи и группы – lusrmgr.msc;
– мастер передачи файлов Bluetooth – fsquirt;
– настройка системы – msconfig;
– назначенные задания – control schedtasks;
– общие папки – fsmgmt.msc;
– общие ресурсы DDE – ddeshare;
– папка обмена – clipbrd;
– проверка подписи файла – sigverif;
– программа сетевого клиента SQL – cliconfg;
– производительность – perfmon.msc;
– просмотр событий – eventvwr.msc;
– подключение к рабочему столу – mstsc;
– результирующая политика – rsop.msc;
– редактор системных файлов – sysedit;
– реестр – regedit;
– редактор личных символов – eudcedit;
– сертификаты – certmgr.msc;
– служба диагностики DirectX – dxdiag;
– службы – services.msc;
– службы компонентов – dcomcnfg;

– служба индексирования – ciadv.msc;
– съемные ЗУ – ntmsmgr.msc;
– телнет – telnet;
– управление дисками – diskmgmt.msc;
– управление рабочим столом – mstscoo;
– управление компьютером – compmgmt.msc;
– удаление вредоносных программ – mrt.exe.

Устранение возможных ошибок системы при включении брандмауэра. При возникновении ошибок при попытке включить брандмауэр, например как на рис. 14, необходимо включить брандмауэр в соответствующих службах Windows (рис. 15–17).

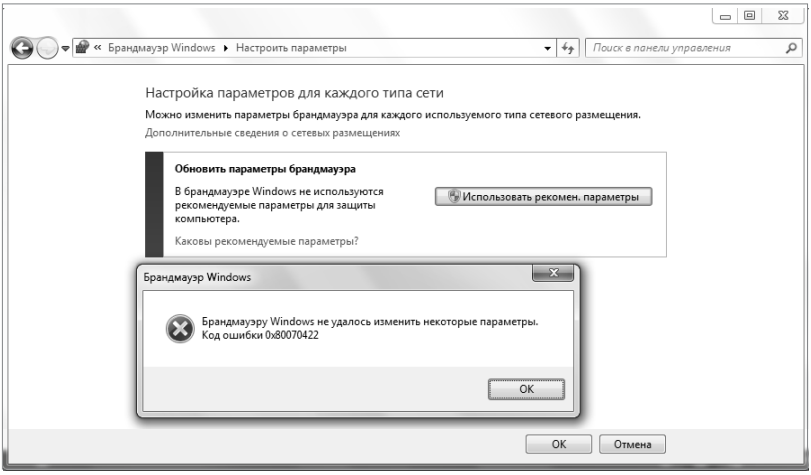

Рис. 14. Ошибка при попытке включить брандмауэр

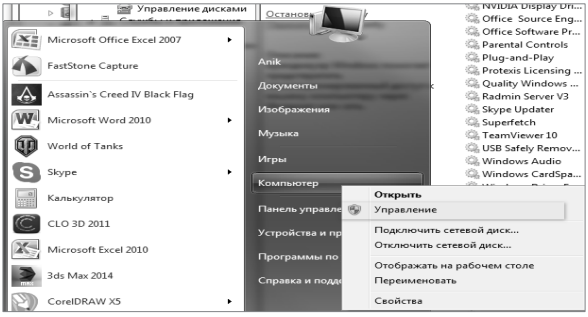

Рис. 15. Открытие окна «Управление»

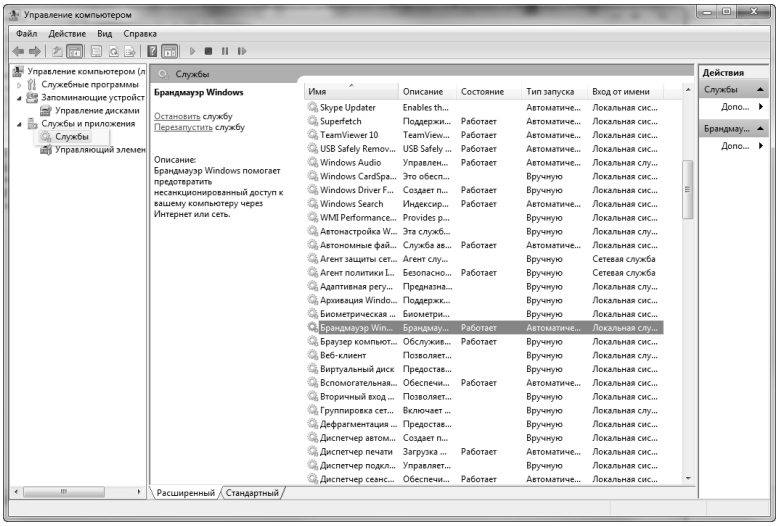

Рис. 16. Доступ к службе «Брандмауэр»

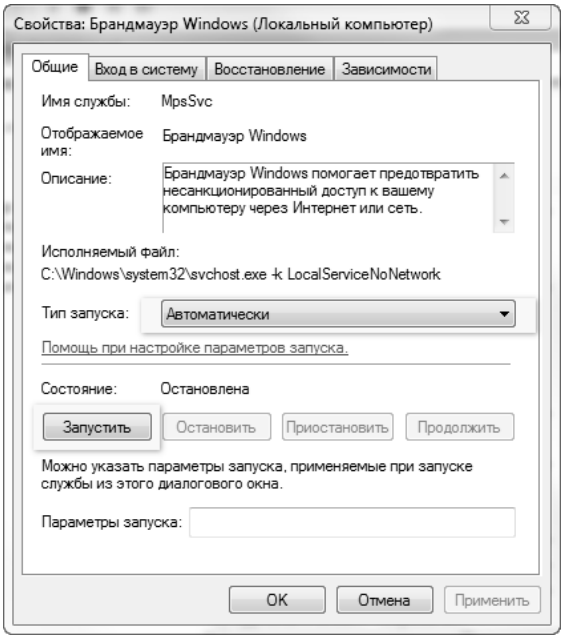

Рис. 17. Запуск брандмауэра

Контрольные вопросы

1. Дайте определение понятию «брандмауэр».

2. Каково основное назначение брандмауэра?

3. Как создаются правила по ограничению доступа программ к сети?

4. Как можно вызвать командную строку?

5. Перечислите способы устранения возможных ошибок системы при включении брандмауэра.

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания.

2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).

3. Условие задания (индивидуальный вариант задания).

4. Исполнительская часть.

5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Создайте правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):

а) для одной программы (по выбору) на блокировку подключения;

б) для одной программы (по выбору) на разрешение подключения.

2. Создайте правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):

а) для одной программы (по выбору) на блокировку подключения;

б) для одной программы (по выбору) на разрешение подключения.

3. Верните настройки брандмауэра в исходное состояние до начала выполнения практического задания.

4. Опробуйте действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).

Практическое занятие № 5

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ

Цель: овладеть основными криптографическими алгоритмами симметричного шифрования.

Теоретические сведения

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Помимо этого, современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

В англоязычной литературе зашифрование/расшифрование – enciphering/deciphering.

Классификация алгоритмов шифрования:

1) симметричные (с секретным, единым ключом, одноключевые, single-key):

1.1) потоковые:

– с одноразовым или бесконечным ключом (infinite-key cipher);

– с конечным ключом;

– на основе генератора псевдослучайных чисел;

1.2) блочные:

– шифры перестановки (permutation, P-блоки);

– шифры замены (substitution, S-блоки):

а) моноалфавитные;

б) полиалфавитные;

2) асимметричные (с открытым ключом, public-key):

– Диффи – Хеллмана (DH – Diffie, Hellman);

– Райвеста – Шамира – Адлемана (RSA – Rivest, Shamir, Adleman);

– Эль-Гамаля (ElGamal).

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в три этапа:

– отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);

– отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;

– получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

– шифры перестановки (transposition, permutation, P-блоки);

– шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Различают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

– моноалфавитные (код Цезаря);

– полиалфавитные (шифр Виженера, цилиндр Джефферсона, диск Уитстона, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например, в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций (рис. 18).

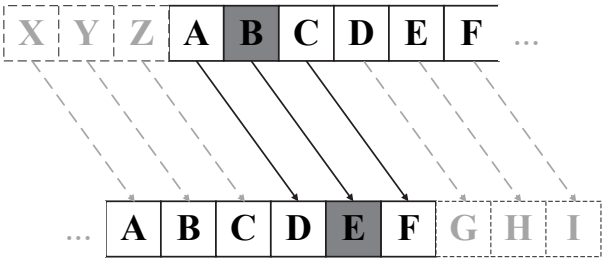

Рис. 18. Пример шифра Цезаря

Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Он более стойкий, чем шифратор, использующий только замены или перестановки.

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания – другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией такова:

– получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

– отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

– получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

Контрольные вопросы

1. Что такое криптография?

2. В чем особенность симметричных криптосистем?

3. Что можно использовать в качестве ключа в симметричных криптосистемах?

4. Как происходит расшифровка сообщений в системе Виженера?

5. Расскажите об алгоритме шифрования «двойной квадрат» Уитстона.

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания.

2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).

3. Условие задания.

4. Исполнительская часть.

5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Изучите теоретические сведения по данной теме.

2. Зашифруйте сообщение с использованием нижеперечисленных шифров и полученного секретного ключа (по номеру варианта (см. номер студента в журнале группы) и ключевому слову «Защита»):

– шифр Цезаря;

– шифр Трисемуса;

– шифр Плейфейра;

– шифр Виженера.

В качестве сообщения используйте свое полное имя (Фамилия Имя Отчество).

3. Расшифруйте сообщения по индивидуальному заданию.

<table>
<tr><th>Номер варианта</th><th>Сообщение</th><th>Способ</th></tr>
<tr><td>1</td><td>Ие михежцчжшйч сшихуцчб</td><td>Расшифровать с помощью шифра Цезаря. Ключ 5</td></tr>
<tr><td>2</td><td>съчпщг окхчхиге ичлкпщг</td><td>Расшифровать с помощью шифра Цезаря. Ключ 7</td></tr>
<tr><td>3</td><td>ьоъщочто т лечшыхтлшыьё</td><td>Расшифровать с помощью шифра Цезаря. Ключ 10</td></tr>
<tr><td>4</td><td>Лжбзеииеизиачзнр</td><td>Расшифровать с помощью магического квадрата
<table><tr><td>7</td><td>12</td><td>1</td><td>14</td></tr><tr><td>2</td><td>13</td><td>8</td><td>11</td></tr><tr><td>16</td><td>3</td><td>10</td><td>5</td></tr><tr><td>9</td><td>6</td><td>15</td><td>4</td></tr></table></td></tr>
<tr><td>5</td><td>тяеонаыбиьсрль_т</td><td>Расшифровать с помощью магического квадрата
<table><tr><td>9</td><td>16</td><td>2</td><td>7</td></tr><tr><td>6</td><td>3</td><td>13</td><td>12</td></tr><tr><td>15</td><td>10</td><td>8</td><td>1</td></tr><tr><td>4</td><td>5</td><td>11</td><td>14</td></tr></table></td></tr>
<tr><td>6</td><td>иоарткдпвл_натоа</td><td>Расшифровать с помощью магического квадрата
<table><tr><td>7</td><td>12</td><td>1</td><td>14</td></tr><tr><td>2</td><td>13</td><td>8</td><td>11</td></tr><tr><td>16</td><td>3</td><td>10</td><td>5</td></tr><tr><td>9</td><td>6</td><td>15</td><td>4</td></tr></table></td></tr>
<tr><td>7</td><td>гэ ишн зижшпэг оюжи</td><td>Расшифровать с помощью шифра Цезаря. Ключ 8. Ключевое слово – ВЕСНА</td></tr>
<tr><td>8</td><td>дороюё дъ нозбъвё жодщйц</td><td>Расшифровать с помощью шифра Цезаря. Ключ 5. Ключевое слово – ОСЕНЬ</td></tr>
<tr><td>9</td><td>жъйтаъъщ ёъръ клъюё жёйлал</td><td>Расшифровать с помощью шифра Цезаря. Ключ 6. Ключевое слово – ЗИМА</td></tr>
<tr><td>10</td><td>Боитдиултоьтдгьпсеоснояшмяил_ьубу_дччуч_</td><td>Расшифровать с помощью метода простой перестановки. Таблица 6×7</td></tr>
<tr><td>11</td><td>гг_ _ ипоомитрдр_ос,яубогп_мба дираоитнла_гноаавуоа</td><td>Расшифровать с помощью метода простой перестановки. Таблица 7×7</td></tr>
<tr><td>12</td><td>нотеч_е_ _кем_кчалемре,осеал_в тссоаеотив_к_</td><td>Расшифровать с помощью метода простой перестановки. Таблица 6×7</td></tr>
<tr><td>13</td><td>_яетож_нксучнтуотдеыужбьатй дны_,с_ао_о_яс,_ндк,е_иаиу_кк дднда руто_а_еди.в_нта_ _ахе:_</td><td>Расшифровать с помощью одиночной перестановки по ключу. Ключ – СЧАСТЬЕ. Таблица 12×7</td></tr>
</table>

Номер варианта	Сообщение	Способ
14	Онлгвишлеиоутньмшттьишньо_ _мио_всп_нгоиеодсичтгзнтеесо дев _няднможь_не_ _и_жяеб	Расшифровать с помощью одиночной перестановки по ключу. Ключ – ОКТЯБРЬ. Таблица 11×7
15	_ _еоовипи_ _ _ы_о_ввв_тттыыыт уоо_ _ _атмтерем_у,сес,б_ _тшт _ычкьиьгттт,л,дь	Расшифровать с помощью одиночной перестановки по ключу. Ключ – ФЕВРАЛЬ. Таблица 10×7
16	НТЕЬСЯЛББЫРТОИА_	Расшифровать с помощью двойной перестановки по ключу. Ключ 1 – Мама. Ключ 2 – 3142
17	И_ЛБКЧУОПЧТУ_ОЬР	Расшифровать с помощью двойной перестановки по ключу. Ключ 1 – ЛЕТО. Ключ 2 – 4213
18	АМУМАФАССИ_ТКРК_	Расшифровать с помощью двойной перестановки по ключу. Ключ 1 – ЗИМА. Ключ 2 – 2341
19	ъгчгл кыпргл бгнщзг	Расшифровать с помощью шифра Трисемуса. Ключ – ПРАВИТЕЛЬ
20	иецеж пецен, пй ыд зещеъез	Расшифровать с помощью шифра Трисемуса. Ключ – МОСКВА
21	зчгы очхей, й зчгы гйък щчрейв	Расшифровать с помощью шифра Трисемуса. Ключ – МИНСК
22	нп тр яч дн ка бо ат дъ ка цр кб щг уф уч тб ты	Расшифровать с помощью шифра Плейфейра. Ключ – АБСТРАКЦИЯ
23	вт пм зл ко ту нщ кж ек да ъл тс дш ыд пц къ ац ми лф	Расшифровать с помощью шифра Плейфейра.Ключ – РЕПЛИКАЦИЯ
24	рп пд оф бл гщ мф ыи мф цг гн оп см тп гн въ ив жя	Расшифровать с помощью шифра Плейфейра. Ключ – КЛАССИФИКАЦИЯ
25	у ь т ц в ю к п ч ю ч у в у и з к щ й ю т у ф б х к ф э у е в д б е ь б ч о	Расшифровать с помощью шифра Виженера. Ключ – ВЕТЕР
26	д с я ш о ж у в я и х ь с я с б е у ю т в х я ю т к ф я ъ и о е п я	Расшифровать с помощью шифра Виженера. Ключ – ВЕСНА
27	х ш п ф и с ъ ш а с ъ м щ ю ш х ю к п я ц д ю о ы г х з г и ь р с щ с с у х щ м ь т п	Расшифровать с помощью шифра Виженера. Ключ – ПРИЗМА
28	кл ез рц ьй уа бц пв вй ая хй ущ хй бш	Расшифровать с помощью шифра «двойной квадрат» Уитстона. Ключ 1 – ХАЛЯВА. Ключ 2 – РАБОТА
29	пх кю гй яг зо ад зн йр юм тш кь	Расшифровать с помощью шифра «двойной квадрат» Уитстона. Ключ 1 – ХАЛЯВА. Ключ 2 – РАБОТА
30	ба хи хх ьй ля сс эж ап це ък бш	Расшифровать с помощью шифра «двойной квадрат» Уитстона. Ключ 1 – ХАЛЯВА. Ключ 2 – РАБОТА

Практическое занятие № 6

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМОВ АСИММЕТРИЧНОГО ШИФРОВАНИЯ

Цель: овладеть основными криптографическими алгоритмами асимметричного шифрования.

Теоретические сведения

В 1970-х гг. появилась новая система шифрования, называемая шифрованием на ассиметричном (открытом) ключе. Она ассиметрична, потому что не требует использования идентичных ключей отправителем и получателем шифрованного сообщения. Она является системой с открытым ключом, так как один из ключей не содержится в секрете.

Ассиметричная система шифрования использует **открытый ключ**, который передается по открытому каналу и предназначен для шифрования сообщения.

Шифрование на открытом ключе базируется на двух различных ключах, составляющих пару, но не идентичных. В шифровании с асимметричным ключом каждый ключ является уникальным. Пара ключей «открытый/секретный» работает сообща: один ключ предназначен для шифрования данных, а другой – для расшифровки, и наоборот. Секретный ключ должен содержаться в секретности в целях безопасности, а открытый ключ может передаваться по небезопасному соединению без угрозы для системы. Следовательно, система шифрования на открытом ключе решает одну из главных проблем старых систем шифрования, заключающуюся в безопасном способе передачи ключа шифрования другой стороне.

Как правило, открытые ключи используются только для зашифровки данных. Расшифровать их сможет только тот пользователь, чей компьютер содержит соответствующий секретный ключ. Эта система построена на математических принципах, используемых в шифрах с открытыми ключами и обеспечивающих существование

одного и только одного уникального секретного ключа, соответствующего уникальному открытому ключу. Следовательно, если выполняется шифрование данных пользователя на общем ключе, можно быть уверенным, что только пользователь, владеющий второй, секретной, половиной ключа, сможет их расшифровать (рис. 19).

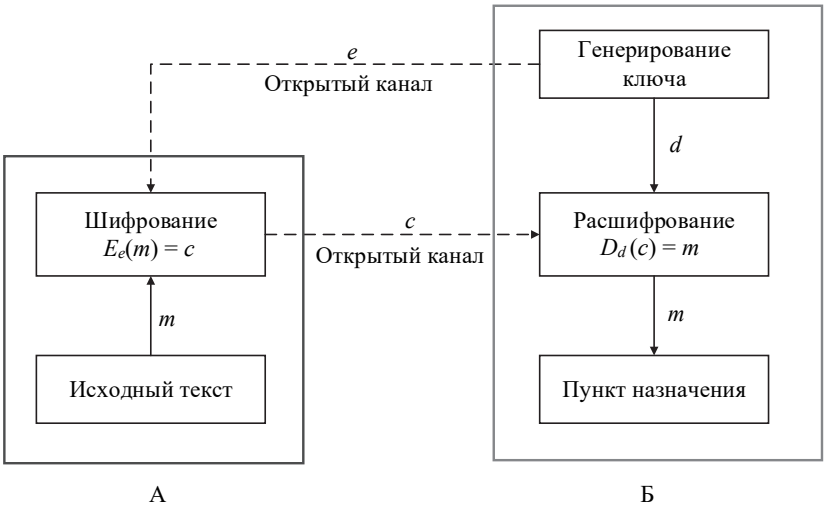

Рис. 19. Схема шифрования

Данная система шифрования основана на идее **односторонней функции,** т. е. такой функции $f(x)$, что по известному x довольно просто найти значение $f(x)$, тогда как определение x из $f(x)$ невозможно за разумный срок.

Пусть e и d – ключи шифрования и расшифрования соответственно; E_e – функция шифрования; D_d – функция расшифрования.

Пользователь Б выбирает пару (e, d) и шлет ключ шифрования e (открытый ключ) пользователю А по открытому каналу, а ключ расшифрования d (закрытый ключ) защищен и секретен (он не должен передаваться по открытому каналу).

Чтобы послать сообщение m пользователю Б, пользователь А применяет функцию шифрования, определенную открытым ключом e: $E_e(m) = c$, где c – полученный шифротекст.

Пользователь Б расшифровывает шифротекст c, применяя обратное преобразование D_d, однозначно определенное значением d.

Реализация элементов криптосистемы RSA. RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и др.

Весь алгоритм расписан в табл. 1.

Таблица 1

Алгоритм RSA

Этап	Описание операции	Результат операции
Генерация ключей	Выбрать два простых различных числа	$p = 3557$ $q = 2579$
	Вычислить модуль (произведение)	$n = p \cdot q = 3557 \cdot 2579 = 9\ 173\ 503$
	Вычислить функцию Эйлера	$\varphi(n) = (p-1)(q-1) = 9\ 167\ 368$
	Выбрать открытую экспоненту	$e = 3$
	Вычислить секретную экспоненту	$d = e^{-1} \bmod \varphi(n)$ $d = 6\ 111\ 579$
	Опубликовать открытый ключ	$\{e, n\} = \{3, 9\ 173\ 503\}$
	Сохранить закрытый ключ	$\{d, n\} = \{6\ 111\ 579, 9\ 173\ 503\}$
Шифрование	Выбрать текст для зашифровки	$m = 111\ 111$
	Вычислить шифротекст	$c = E(m) = m^e \bmod n = 111\ 111^3 \times$ $\times \bmod 9\ 173\ 503 = 4\ 051\ 753$
Расшифрование	Вычислить исходное сообщение	$m = D(c) = c^d \bmod n = 4\ 051\ 753^{6\ 111\ 579} \times$ $\times \bmod 9\ 173\ 503 = 111\ 111$

Алгоритмы криптосистемы с открытым ключом можно использовать:

– как самостоятельное средство для защиты передаваемой и хранимой информации;

– как средство распределения ключей;

– как средство аутентификации пользователей.

Недостатки в сравнении с симметричными системами:

– шифрование/расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование/расшифрование того же текста симметричным алгоритмом;

– требуются существенно бóльшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами;

– в алгоритм сложнее внести изменения;

– хотя сообщения надежно шифруются, получатель и отправитель самим фактом пересылки шифрованного сообщения «засвечиваются»;

– более длинные ключи.

Ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью (табл. 2).

Таблица 2

Сопоставление длины ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью

Длина симметричного ключа, бит	Длина ключа RSA, бит
56	384
64	512
80	768
112	1792
128	2304

Реализация элементов схемы шифрования Эль-Гамаля.

Генерация ключей:

1) генерируется случайное простое число p длиной n битов;

2) выбирается случайный примитивный элемент g;

3) выбирается случайное целое число x такое, что $1 < x < p - 1$;

4) вычисляется по формуле (16):

$$y = g^x \bmod p; \tag{16}$$

5) открытым ключом является тройка (p, g, y), закрытым ключом – число x.

Шифрование. Сообщение M шифруется следующим образом:

1) выбирается сессионный ключ – случайное целое число k такое, что $1 < k < p - 1$;

2) вычисляются числа a и b по формулам (17) и (18) соответственно:

$$a = g^k \bmod p; \tag{17}$$

$$b = y^k M \bmod p; \tag{18}$$

3) пара чисел (a, b) является шифротекстом.

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

Расшифрование. Зная закрытый ключ x, исходное сообщение можно вычислить из шифротекста (a, b) по формуле (19):

$$M = b(a^x)^{-1} \bmod p. \tag{19}$$

По формуле (20) нетрудно проверить, что

$$(a^x)^{-1} = g^{-kx} \bmod p. \tag{20}$$

Поэтому, согласно формуле (21):

$$b(a^x)^{-1} \equiv y^k M g^{-xk} \equiv g^{xk} M g^{-xk} \equiv M \bmod p. \tag{21}$$

Для практических вычислений больше подходит формула (22):

$$M = b(a^x)^{-1} \bmod p = b \cdot a^{(p-1-x)} \bmod p. \tag{22}$$

Шифрование. Допустим, что нужно зашифровать сообщение $M = 5$.

Произведем генерацию ключей.

Пусть $p = 11$, $g = 2$. Выберем $x = 8$ – случайное целое число x такое, что $1 < x < p$.

Вычислим y по формуле (23):

$$y = g^x \bmod p = 2^8 \bmod 11 = 3. \tag{23}$$

Итак, открытым ключом является тройка (p, g, y) = (11, 2, 3), а закрытым – число $x = 8$.

Выбираем случайное целое число k такое, что $1 < k < (p - 1)$. Пусть $k = 9$.

Вычисляем a по формуле (24):

$$a = g^k \bmod p = 2^9 \bmod 11 = 512 \bmod 11 = 6. \quad (24)$$

Вычисляем b по формуле (25)

$$a = y^k M \bmod p = 3^9 \cdot 5 \bmod 11 = 19\,683 \cdot 5 \bmod 11 = 9. \quad (25)$$

Полученная пара $(a, b) = (6, 9)$ является шифротекстом.

Расшифрование. Необходимо получить сообщение $M = 5$ по известному шифротексту $(a, b) = (6, 9)$ и закрытому ключу $x = 8$.

Вычисляем M по формуле (26):

$$M = b(a^x)^{-1} \bmod p = 9 \cdot (6^8)^{-1} \bmod 11 = 5. \quad (26)$$

Получили исходное сообщение $M = 5$.

Реализация элементов схемы шифрования Диффи – Хеллмана. В 1976 г. после публичной критики алгоритма DES и указания на сложность обработки секретных ключей Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) опубликовали свой алгоритм обмена ключами. Это была первая публикация на тему криптографии с открытым ключом и, возможно, самый большой шаг вперед в области криптографии, сделанный когда-либо.

Из-за невысокого быстродействия, свойственного асимметричным алгоритмам, алгоритм Диффи – Хеллмана не предназначен для шифрования данных. Он был ориентирован на передачу секретных ключей DES, ARS или других подобных алгоритмов через небезопасную среду. В большинстве случаев алгоритм Диффи – Хеллмана не используется для шифрования сообщений, потому что он, в зависимости от реализации, от 10 до 1000 раз медленнее алгоритма DES.

До алгоритма Диффи – Хеллмана было сложно совместно использовать зашифрованные данные из-за проблем хранения ключей и передачи информации. В большинстве случаев передача информации по каналам связи небезопасна, потому что сообщение может пройти десятки систем, прежде чем оно достигнет потенциального адресата, и нет никаких гарантий, что по пути никто не сможет

взломать секретный ключ. Уитфилд Диффи и Мартин Хеллман предложили зашифровывать секретный ключ DES по алгоритму Диффи – Хеллмана на передающей стороне и пересылать его вместе с сообщением, зашифрованным с использованием DES. Тогда на другом конце его сможет расшифровать только получатель сообщения.

На практике **обмен ключами** по алгоритму Диффи – Хеллмана происходит по следующей схеме.

1. Два участника обмена договариваются о двух числах. Один выбирает большое простое число, а другой – целое число, меньшее числа первого участника. Переговоры они могут вести открыто, и это никак не отразится на безопасности.

2. Каждый из двух участников, независимо друг от друга, генерирует другое число, которое они будут хранить в тайне. Эти числа выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участнику обмена, и он играет роль открытого ключа.

3. Участники обмена обмениваются открытыми ключами. Далее они, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляют ключ сессии. Каждый партнер вычисляет один и тот же ключ сессии.

4. Ключ сессии может использоваться как секретный ключ для другого алгоритма шифрования, например DES. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

Самое сложное в алгоритме Диффи – Хеллмана обмена ключами – это понять, какие два различных независимых цикла шифрования используются. Алгоритм Диффи – Хеллмана применяется для обработки небольших сообщений от отправителя получателю. Но в этом маленьком сообщении передается секретный ключ для расшифровки большого сообщения.

Сильная сторона алгоритма – никто не сможет скомпрометировать секретное сообщение, зная один или даже два открытых ключа получателя и отправителя. В качестве секретных и открытых ключей используются очень большие целые числа. Алгоритм Диффи – Хеллмана основан на полезных для криптографии свойствах дискретных логарифмов.

Рассмотрим пример. Пользователь Е – криптоаналитик. Он читает пересылку пользователей Б и А, но не изменяет содержимого

их сообщений. В табл. 3 представлены данные, которые знает либо не знает пользователь А:

- s = секретный ключ, $s = 2$;
- g = простое число, меньшее p, $g = 5$;
- p = открытое простое число, $p = 23$;
- a = секретный ключ пользователя А, $a = 6$;
- A = открытый ключ пользователя А, $A = g\ a \bmod p = 8$;
- b = секретный ключ пользователя Б, $b = 15$;
- B = открытый ключ пользователя Б, $B = g\ b \bmod p = 19$.

Таблица 3

Данные пользователя А

Знает	Не знает
$p = 23$ $g = 5$ $a = 6$ $A = 5^6 \bmod 23 = 8$ $B = 5^b \bmod 23 = 19$ $s = 19^6 \bmod 23 = 2$ $s = 8^b \bmod 23 = 2$ $s = 19^6 \bmod 23 = 8^b \bmod 23$ $s = 2$	$b = ?$

В табл. 4, 5 представлены данные пользователей Б и Е, аналогично табл. 3 с данными пользователя А.

Таблица 4

Данные пользователя Б

Знает	Не знает
$p = 23$ $g = 5$ $b = 15$ $B = 5^{15} \bmod 23 = 19$ $A = 5^a \bmod 23 = 8$ $s = 8^{15} \bmod 23 = 2$ $s = 19^a \bmod 23 = 2$ $s = 9^{15} \bmod 23 = 19^a \bmod 23$ $s = 2$	$a = ?$

Таблица 5

Данные пользователя Е

Знает	Не знает
$p = 23$ $g = 5$ $A = 5^a \bmod 23 = 8$ $B = 5^b \bmod 23 = 19$ $s = 19^a \bmod 23$ $s = 8^b \bmod 23$ $s = 19^a \bmod 23 = 8^b \bmod 23$	$a = ?$ $b = ?$ $s = ?$

Контрольные вопросы

1. В чем особенность асимметричных криптосистем?
2. С помощью какого ключа происходит шифрование сообщения?
3. В чем особенность алгоритма Диффи – Хеллмана?
4. Какие недостатки можно выделить в асимметричных криптосистемах?

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).
2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).
3. Условие задания.
4. Исполнительская часть.
5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Объясните процесс работы алгоритма RSA.
2. Объясните процесс работы алгоритма Диффи – Хеллмана.
3. Объясните процесс работы алгоритма Эль-Гамаля.
4*. Используя существующие криптографические библиотеки, создайте приложение и проанализировать работу вышеперечисленных алгоритмов.

Практическое занятие № 7

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Цель: изучить и закрепить умение реализации электронно-цифровой подписи на примере RSA.

Теоретические сведения

Электронная цифровая подпись. Если обратиться к закону Республики Беларусь «Об электронном документе и электронной цифровой подписи», то можно найти следующее ее определение: «Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию».

Электронная цифровая подпись (ЭЦП) предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой собственноручной подписи.

Далее даны наиболее часто используемые термины.

Открытый текст – данные, подлежащие шифрованию или полученные в результате расшифрования.

Шифртекст – данные, полученные в результате применения шифра к открытому тексту.

Шифр – совокупность обратимых преобразований, зависящая от некоторого параметра (ключа).

Ключ – параметр шифра, определяющий выбор одного преобразования из совокупности.

Факторизация – процесс разложения числа на простые множители.

НОД – наибольший общий делитель.

Числа a и b называются **взаимно простыми**, если НОД этих чисел равен 1.

Функция Эйлера $\varphi(n)$ – функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним.

Использование электронной подписи позволяет осуществить:

– контроль целостности передаваемого документа;

– защиту от изменений (подделки) документа;

– невозможность отказа от авторства;

– доказательное подтверждение авторства документа.

Наиболее известные схемы создания электронной цифровой подписи:

– Диффи – Хеллмана;

– DSA;

– RSA;

– Эль-Гамаля (ElGamal);

– Рабина;

– Шнорра;

– Диффи – Лампорта.

На рис. 20 представлена общая схема алгоритма шифрования Диффи – Хеллмана.

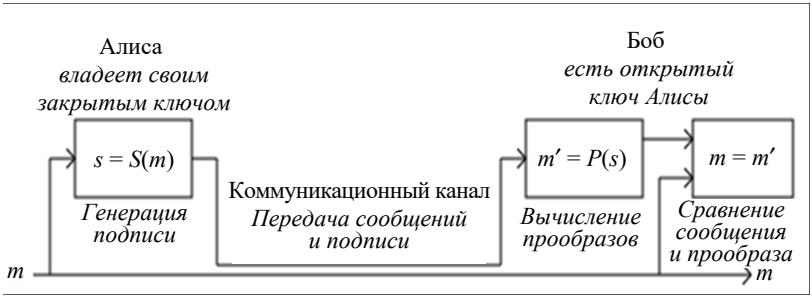

Рис. 20. Схема работы алгоритма Диффи – Хеллмана

Схема использования алгоритма RSA при большом модуле N практически не позволяет злоумышленнику получить закрытый ключ и прочитать зашифрованное сообщение. Однако она дает возможность злоумышленнику подменить сообщение от абонента А к абоненту Б, так как абонент А шифрует свое сообщение открытым ключом, полученным от Б по открытому каналу связи. А раз открытый ключ передается по открытому каналу, любой может получить его и использовать для подмены сообщения. Избежать этого можно, используя более сложные протоколы, например следующий.

Пусть, как и раньше, пользователь А хочет передать пользователю Б сообщение, состоящее из нескольких блоков m_i. Перед началом сеанса связи абоненты генерируют открытые и закрытые ключи, обозначаемые, как указано в табл. 6.

Таблица 6

Генерация открытого и закрытого ключа абонента

Пользователь	Открытый ключ	Закрытый ключ
А	$N_А$, $d_А$	$e_А$
Б	$N_Б$, $d_Б$	$e_Б$

В результате каждый пользователь имеет свои собственные открытый (состоящий из двух частей) и закрытый ключи. Затем пользователи обмениваются открытыми ключами. Это подготовительный этап протокола.

Основная часть протокола состоит из следующих шагов.

1. Сначала пользователь А вычисляет числа c_i по формуле (27), т. е. шифрует сообщение своим закрытым ключом:

$$c_i = m_i^{e_А} \bmod N_А. \tag{27}$$

В результате этих действий пользователь А подписывает сообщение.

2. Затем пользователь А вычисляет числа g_i по формуле (28), т. е. шифрует то, что получилось на шаге 1, открытым ключом пользователя Б:

$$g_i = c_i^{d_Б} \bmod N_Б. \tag{28}$$

На этом этапе сообщение шифруется, чтобы никто посторонний не мог его прочитать.

3. Последовательность чисел g_i передается пользователю Б.

4. Пользователь Б получает g_i и вначале вычисляет последовательность числа c_i по формуле (29), используя свой закрытый ключ:

$$c_i = g_i^{e_Б} \bmod N_Б. \tag{29}$$

При этом сообщение расшифровывается.

5. Затем пользователь Б определяет числа m_i по формуле (30), используя открытый ключ пользователя А:

$$m_i = c_i^{d_А} \bmod N_А. \tag{30}$$

За счет выполнения этого этапа проводится проверка подписи пользователя А.

В результате абонент Б получает исходное сообщение и убеждается в том, что его отправил именно абонент А. Данная схема позволяет защититься от нескольких видов возможных нарушений:

– пользователь А не может отказаться от своего сообщения, если он признает, что секретный ключ известен только ему;

– нарушитель без знания секретного ключа не может ни сформировать, ни сделать осмысленное изменение сообщения, передаваемого по линии связи.

Электронная подпись на основе алгоритма RSA. Данная схема позволяет избежать многих конфликтных ситуаций. Иногда нет необходимости зашифровывать передаваемое сообщение, но нужно его скрепить электронной подписью. В этом случае из приведенного выше протокола исключаются шаги 2 и 4, т. е. текст шифруется закрытым ключом отправителя, и полученная последовательность присоединяется к документу. Получатель с помощью открытого ключа отправителя расшифровывает прикрепленную подпись, которая, по сути, является зашифрованным повторением основного сообщения. Если расшифрованная подпись совпадает с основным текстом, значит, подпись верна.

Существуют и другие варианты применения алгоритма RSA для формирования ЭЦП. Например, можно шифровать (т. е. подписывать) открытым ключом не само сообщение, а хеш-код от него.

Возможность применения алгоритма RSA для получения электронной подписи связана с тем, что секретный и открытый ключи в этой системе равноправны. Каждый из ключей (d или e) может использоваться как для шифрования, так и для расшифрования. Это свойство выполняется не во всех криптосистемах с открытым ключом.

Алгоритм RSA может применяться также и для обмена ключами.

Реализация элементов ЭЦП RSA. Протоколы ЭЦП, с одной стороны, относят к протоколам аутентификации, так как они гарантируют, что сообщение поступило от достоверного отправителя, а с другой стороны – к протоколам контроля целостности, так как они гарантируют, что сообщение пришло в неискаженном виде. Более того, получатель в дальнейшем может использовать ЭЦП как доказательство достоверности сообщения третьим лицам (арбитру)

в том случае, если отправитель впоследствии попытается отказаться от него.

Говоря о схеме цифровой подписи, обычно имеют в виду следующую классическую ситуацию:

– отправитель знает содержание сообщения, которое он подписывает;

– получатель, зная открытый ключ проверки подписи, может проверить правильность подписи полученного сообщения в любое время без какого-либо разрешения и участия отправителя;

– безопасность схемы подписи гарантируется.

При создании цифровой подписи по классической схеме отправитель:

– применяет к исходному сообщению T хеш-функцию $h(T)$ и получает хеш-образ r сообщения;

– вычисляет цифровую подпись s по хеш-образу r с использованием своего закрытого ключа;

– посылает сообщение T вместе с цифровой подписью s получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

– применяет к полученному сообщению T хеш-функцию $h(T)$ и получает хеш-образ h сообщения;

– расшифровывает хеш-образ h' из цифровой подписи s с использованием открытого ключа отправителя;

– проверяет соответствие хеш-образов h и h', и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

Как видно из этой схемы, порядок использования ключей обратный тому, который используется при передаче секретных сообщений. Вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

Рассмотрим данный процесс поэтапно.

Этап 1. Выработка ключей (выполняет отправитель А) – см. практическую работу № 6 «Криптографическая защита информации с помощью алгоритмов асимметричного шифрования».

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель А) (табл. 7).

Таблица 7

Отправка сообщения и ЭЦП на базе алгоритма RSA

Описание операции	Пример
1. Вычисление хеш-образа $h = h(T)$, где T – исходное сообщение, $h(T)$ – хеш-функция (для MD5 длина хеш-образа 128 бит)	$h = 7$
2. Выработка цифровой подписи $s = h^d \bmod n$, где d – закрытый ключ отправителя А, n – часть открытого ключа отправителя А	$s = 7^{29} \bmod 91 = 63$
3. Отправка получателю Б исходного сообщения T и цифровой подписи s	–

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель Б) (табл. 8).

Таблица 8

Получение сообщения и проверка ЭЦП на базе алгоритма RSA

Описание операции	Пример
1. Вычисление хеш-образа по полученному сообщению $h' = h(T')$, где T' – полученное сообщение. Если $T = T'$, то должно быть $h = h'$	$h' = 7$
2. Вычисление хэш-образа из цифровой подписи $h'' = s^e \bmod n$, где e и n – открытый ключ отправителя А.	$h'' = 73^{29} \bmod 91 = 7$
3. Так как $h' = h''$, то получатель Б делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено А	–

Разновидности ЭЦП. Кроме классической схемы ЭЦП различают еще несколько специальных:

– схема «конфиденциальной» (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;

– схема подписи «вслепую» («затемненной» подписи) – отправитель не знает подписанного им сообщения;

– схема «мультиподписи» – вместо одного отправителя сообщение подписывает группа из нескольких участников;

– схема «групповой» подписи – получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано.

В то же время, в случае необходимости, отправитель может быть определен.

Отметим некоторые **недостатки алгоритма цифровой подписи RSA.**

1. При вычислении ключей для системы цифровой подписи RSA необходимо проверять ряд дополнительных условий. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение.

2. Для обеспечения криптостойкости цифровой подписи RSA по отношению к попыткам фальсификации, например на уровне алгоритма шифрования DES, необходимо использовать при вычислениях ключей очень большие целые числа, что требует значительных вычислительных затрат, превышающих на 20–30% вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости.

3. Цифровая подпись RSA уязвима к так называемой мультипликативной атаке. Иначе говоря, алгоритм цифровой подписи RSA позволяет злоумышленнику без знания секретного ключа сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов.

Контрольные вопросы

1. Дайте определение понятию «электронная цифровая подпись».

2. Объясните порядок использования ключей (открытый, закрытый) при отправке и проверке ЭЦП.

3. Перечислите специальные схемы ЭЦП.

4. Назовите недостатки алгоритма цифровой подписи RSA.

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).

2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).

3. Условие задания.

4. Исполнительская часть.

5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Объясните последовательность выполнения процедур генерации и проверки ЭЦП.

2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.

3. Опишите схему протокола ЭЦП на основе алгоритма RSA.

4*. На базе алгоритма RSA получите ЭЦП (в проекте можно использовать существующие криптографические алгоритмы). Удостоверьтесь, что ЭЦП принадлежит именно этому сообщению.

Практическое занятие № 8

ТЕОРИЯ ЧИСЕЛ

Цель: получить основные сведения из курса теории чисел.

Теоретические сведения

Рассмотрим N – множество натуральных чисел. Множество целых чисел Z – счетное, состоит из элементов 0; ±1; ±2; …; ±n, … . На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых $a, b, c \in Z$):

1) ассоциативность: $a + (b + c) = (a + b) + c$; $a \cdot (b \cdot c) = a \cdot (b \cdot c)$;

2) коммутативность: $b + a = a + b$; $a \cdot b = b \cdot a$;

3) существует нейтральный элемент – 0 и 1 соответственно: $a + 0 = 0 + a = a$; $a \cdot 1 = 1 \cdot a = a$;

4) $(a + b) \cdot c = a \cdot c + b \cdot c$ – дистрибутивность;

5) для каждого целого $a \in Z$ существует единственное противоположное, т. е. такое целое b, что $a + b = b + a = 0$.

Теорема 1 (*о делении с остатком*). Для любых целых чисел a и b, $b \neq 0$, существует единственные целые числа q и r, $0 \leq r < b$, такие, что $a = b \cdot q + r$.

В этом равенстве r называют остатком, а q – частным (неполным частным – при $r \neq 0$) от деления a на b. При $r = 0$ величины b и q называют делителями или множителями числа a.

Следствие. Пусть b – натуральное число, $b > 1$. Для всякого целого числа a и максимального целого $m \geq 0$ с условием $a > b^m$ существуют единственные целые a_i, $0 \leq i < b$, такие, что $a = \pm(a_m b^m + a_{m-1} b^{m-1} + \ldots + a_0)$.

Такое равенство записывают сокращенно $a = \pm(a_m a_{m-1} \ldots a_0)_b$ или $a = \pm a_m a_{m-1} \ldots a_0$ (если b известно по контексту) и называют записью числа a в b-ичной позиционной системе счисления или системе счисления по основанию b. Нам кажется естественной привычная десятичная позиционная система записи целых чисел ($b = 10$). В различных ситуациях более удобными оказываются другие основания. К примеру, во всех компьютерах на микроуровне вычисления

проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную – 16-ричную систему счисления.

Лемма 1. Если в равенстве $a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_m$ все слагаемые – целые числа и все, кроме может быть одного, делятся на целое d, то и это исключенное слагаемое делится на d.

Определение 1. Если целые числа $a_1, a_2, \ldots, a_n$ делятся на целое d, то d называют их *общим делителем*.

В дальнейшем речь идет только о положительных целых делителях.

Определение 2. Максимальный из общих делителей целых чисел $a_1, a_2, \ldots, a_n$ называется их *наибольшим общим делителем* и обозначается через НОД $(a_1, a_2, \ldots, a_n)$.

Теорема 2. Если $a = b \cdot q + c$, то НОД (a, b) = НОД (b, c).

Теорема 2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема 3. Наибольший общий делитель целых чисел a и b $(a > b)$ равен последнему отличному от нуля остатку цепочки равенств:

$a = b \cdot q_1 + r_1$;

$b = b \cdot q_2 + r_2$;

……

$r_{n-2} = r_{n-1} \cdot q_n + r_n$;

$r_{n-1} = r_n \cdot q_{n+1}$,

т. е. r_n = НОД (a, b).

Теорема 3 формулирует алгоритм Евклида нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий – второй способ вычисления наибольшего общего делителя по алгоритму Евклида: вычисляем последовательно разности $a - b = c$, $b - c = d$, … до получения последней ненулевой разности, которая и совпадает с НОД (a, b).

Пример 1. С помощью алгоритма Евклида найти НОД (72, 26).

Решение. В соответствии с теоремой 2 $72 = 26 \cdot 2 + 20$; $26 = 20 \cdot 1 + 6$; $20 = 6 \cdot 3 + 2$; $6 = 2 \cdot 3$. Следовательно, НОД (72, 26) = 2.

Теорема 4. Если d = НОД (a, b), то существуют такие целые u и v, что выполняется следующее соотношение (Безу): $d = au + bv$.

Пример 2. Из примера 1.1 следует, что $2 = 20 + 6 \cdot (-3) = 20 + (26 + 20 \cdot (-1)) \cdot (-3) = 20 \cdot 4 + 26 \cdot (-3) = (72 + 26 \cdot (-2)) \cdot (4 + 26 \cdot (-3)) = 72 \cdot 4 + 26 \cdot (-11)$.

Такой способ получения соотношения Безу для конкретных целых чисел называется расширенным алгоритмом Евклида. Он состоит из двух этапов собственно алгоритма Евклида – прогонки вниз и прогонки вверх последовательного выражения остатков в каждом из шагов предыдущего этапа (с соответствующим приведением подобных на каждом шаге).

Определение 3. Натуральное число $p > 1$ называется *простым*, если оно делится только на 1 и на себя.

Теорема 5. Всякое натуральное число $n > 1$ либо является простым числом, либо имеет простой делитель.

Заметим, что из соотношения $n = p \cdot q$ натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку $[2, \sqrt{n}]$. Легко видеть, что наименьший натуральный делитель $p > 1$ натурального числа $n > 1$ является простым числом. Исторически первый метод проверки натурального числа $n > 1$ на простоту заключается в делении его на простые числа, не превосходящие $\sqrt{n}$, и носит название «решето Эратосфена». К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

Теорема 6 (*Евклида*). Простых чисел бесконечно много.

Значение простых чисел в том, что они по теореме 5 являются составными кирпичиками всех натуральных чисел.

Определение 4. Целые числа a и b называются *взаимно простыми,* если НОД $(a, b) = 1$.

Теорема 7 (*критерий взаимной простоты целых чисел*). Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство $a \cdot u + b \cdot v = 1$.

Следствие. НОД $(ac, b) = 1$ тогда и только тогда, когда НОД $(a, b) = 1$ и НОД $(c, b) = 1$.

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

Лемма 2. Пусть произведение целых чисел ab делится на целое число c и НОД $(a, c) = 1$. Тогда b делится на c.

Теорема 8 (*основная теорема арифметики*). Всякое целое число $n > 1$ однозначно раскладывается в произведение простых множителей:

$n = \pm p_1 \cdot p_2 \cdot \ldots \cdot p_s$.

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа: $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_t^{r_t}$.

Пример 3. Приведем примеры канонических разложений целых чисел:

а) $196 = 2 \cdot 98 = 2 \cdot 2 \cdot 49 = 2^2 \cdot 7^2$;

б) $2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

Теорема 9. Пусть m – натуральное число, $m > 1$. Для любых целых чисел a и b следующие условия равносильны:

1) a и b имеют одинаковые остатки от деления на m;

2) $a - b$ делится на m, т. е. $a - b = mq$ для подходящего целого q;

3) $a = b + mq$ для некоторого целого q.

Определение 5. Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют одному из условий теоремы 9. Этот факт обозначают формулой $a \equiv b \pmod m$ или $a \equiv b(m)$ и называют данную формулу сравнением.

Пример 4. $-5 \equiv 7 \pmod 4 \equiv 11 \pmod 4 \equiv 23 \pmod 4 \equiv 3 \pmod 4$.

Пример 5. Если $a = mq + r$, то $a \equiv r \pmod m$ – всякое целое число сравнимо по модулю m со своим остатком от деления на m. Это следует из определения 5 и второго условия теоремы 9. Ведь $a - r$ делится на m.

Основные свойства сравнений:

1) пусть $a \equiv b \pmod m$. Тогда $(a \pm c) \equiv (b \pm c) \pmod m$ для всякого целого c, т. е. к обеим частям сравнения можно добавить (или вычесть из обеих частей) одно и то же число;

2) сравнения можно почленно складывать и вычитать: если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $(a + c) \equiv (b + d) \pmod m$; $(a - c) \equiv (b - d) \pmod m$;

3) сравнения можно почленно перемножать: если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$;

4) сравнения можно почленно возводить в любую натуральную степень: если $a \equiv b \pmod m$, то $a^n \equiv b^n \pmod m$;

50 если в сравнении $a \equiv b \pmod m$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить: $a/d \equiv b/d \pmod{m/d}$;

6) сравнение можно сократить на общий множитель, взаимно простой с модулем: если $a = ad_1$, $b = bd_1$, НОД $(d, m) = 1$, то из сравнения $ad_1 \equiv bd_1 \pmod m$ следует сравнимость a_1 и b_1 по модулю m: $a_1 \equiv b_1 \pmod m$;

7) сравнение можно умножить на любой целый множитель: если $a \equiv b \pmod m$, то $at \equiv bt \pmod m$ для всякого целого t;

8) рефлексивность: $a \equiv a \pmod m$ для любого целого a и всякого натурального $m > 1$;

9) симметричность: если $a \equiv b \pmod m$, то $b \equiv a \pmod m$;

10) транзитивность: если $a \equiv b \pmod m$, $b \equiv c \pmod m$, то $a \equiv c \pmod m$.

Теорема 10 (*малая теорема Ферма*). Пусть p – простое число, и целое число a не делится на p. Тогда $a^{p-1} \equiv 1 \pmod p$.

Теория сравнений и малая теорема Ферма позволяют быстро находить остаток от деления большого числа на простое число.

Пример 6. Найдем остаток от деления 39^{29} на 31.

Решение. $39 \equiv 8 \pmod{31}$. Поэтому в силу свойства 4 сравнений $39^2 \equiv 8^2 \pmod{31} \equiv 2 \pmod{31}$. Двоичная запись: 29 = 11101. Следовательно, для любого натурального a величина $a^{29} = a^{2^4} \cdot a^{2^3} \cdot a^{2^2} \cdot a$. Далее, $39^4 \equiv 8^4 \pmod{31} \equiv 2^2 \pmod{31}$. Поэтому $39^8 \equiv (39^4)^2 \pmod{31} \equiv 4^2 \pmod{31}$. Тогда $39^{16} \equiv (39^8)^2 \pmod{31} \equiv 16^2 \pmod{31} \equiv 8 \pmod{31}$. Следовательно, $39^{29} \equiv 8 \cdot 16 \cdot 4 \cdot 8 \pmod{31} \equiv 4 \cdot 4 \cdot 8 \pmod{31} \equiv 4 \pmod{31}$. Таким образом, остаток от деления 39^{29} на 31 равен 4.

Примеры решения заданий

Задание 1. Найти канонические разложения чисел $a = 627$, $b = 399$.

Решение.

627	3	399	3
209	11	133	7
19	19	19	19
1		1	

Следовательно, $627 = 3 \cdot 11 \cdot 19$, $399 = 3 \cdot 7 \cdot 19$.

Задание 2. Найти НОД (627, 399) пользуясь:

а) алгоритмом Евклида;

б) разложением чисел на простые множители.

Решение. Применим алгоритм Евклида: $627 = 399 \cdot 1 + 228$; $399 = 228 \cdot 1 + 171$; $228 = 171 \cdot 1 + 57$; $171 = 57 \cdot 3$.

Следовательно, НОД (627; 399) = 57.

Найдем НОД (a, b), воспользовавшись разложением на простые множители чисел a и b, полученным в решении предыдущего задания: $627 = \underline{3} \cdot 11 \cdot \underline{19}$; $399 = \underline{3} \cdot 7 \cdot \underline{19}$. Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих как в одно, так и в другое разложения чисел: НОД (627; 399) = $= \underline{3} \cdot \underline{19} = 57$.

Найдем НОД (a, b) методом вычитаний: 627 – 399 = 228; 399 – – 228 = 171; 228 – 171 = 57; 171 – 57 = 114; 114 – 57 = 57; 57 – 57 = 0. Следовательно, НОД (627; 399) = 57.

Задание 3. С помощью расширенного алгоритма Евклида найти целые числа u, v, удовлетворяющие соотношению Безу: $au + bv =$ = НОД (a, b) для целых чисел $a = 110$; $b = 48$.

Решение. Сначала найдем по алгоритму Евклида НОД (110, 48): $110 = 48 \cdot 2 + 14$; $48 = 14 \cdot 3 + 6$; $14 = 6 \cdot 2 + 2$; $6 = 3 \cdot 2$. Следовательно, НОД (110, 48) = 2.

Теперь построим соотношение Безу для данных a и b. $110 =$ $= 48 \cdot 2 + 14$; поэтому $14 = 110 + 48 \cdot (–2)$; $48 = 14 \cdot 3 + 6$; поэтому $6 = 48 + 14 \cdot (–3)$; $14 = 6 \cdot 2 + 2$; поэтому $2 = 14 + 6 \cdot (–2)$. В это равенство подставим полученное выше выражение для 6 и приведем подобные относительно чисел 48 и 14. Итак, $2 = 14 + 6 \cdot (–2) =$ $= 14 + (48 + 14 \cdot (–3)) \cdot (–2) = 14 \cdot 7 + 48 \cdot (–2)$. В полученное выражение для НОД (110, 48) = 2 подставим вышеприведенное выражение числа 14. Получим окончательно

$$2 = 14 \cdot 7 + 48 \cdot (–2) = (110 + 48 \cdot (–2)) \cdot 7 + 48 \cdot (–2) =$$
$$= 110 \cdot 7 + 48 \cdot (–16) = 2.$$
$$a \quad u \quad b \quad v \quad d.$$

Задание 4. А. Найти остаток от деления 2^{100} на 3.

Решение. 2 делится на 3 с остатком 2, 2^2 делится на 3 с остатком 1. При дальнейшем возведении двойки в степень остатки от деления будут чередоваться 2, 1, 2, 1, 2, … . Значит, в силу четности степени 100 остаток от деления требуемого числа на 3 будет равен 1.

2-й способ – методом сравнений, по аналогии с примером 6. $2^{100} = 4^{50} = (3+1)^{50} \equiv 1^{50} = 1$.

Б. Найти остаток от деления $1989 \cdot 1990 \cdot 1991 + 1992^7$ на 7.

Решение. Заменим каждое число на его остаток от деления на 7:

$$\begin{array}{r|l} 1989 & 7 \\ \hline 14 & 284 \\ 58 & \\ \underline{56} & \\ 29 & \\ \underline{28} & \\ 1 & \end{array} \qquad \begin{array}{r|l} 1990 & 7 \\ \hline 14 & 284 \\ 59 & \\ \underline{56} & \\ 30 & \\ \underline{28} & \\ 2 & \end{array}$$

1991 = 7 · 284 + 3; 1992 = 7 · 284 + 4.

$1 \cdot 2 \cdot 3 + 4^3 = 6 + 64 = 70$. 70 : 7 = 10.

Следовательно, остаток равен нулю.

В. Найти остаток от деления 9^{100} на 8.

Решение. Заменим 9 на его остаток 1 от деления на 8. Имеем $1^{100} = 1$. Значит, остаток от деления 9^{100} на 8 равен 1.

Г. Найти остаток от деления 3^{1989} на 7.

Решение. 3 делится на 7 с остатком 3. 3^2 делится на 7 с остатком 2. Далее достаточно на 3 умножить только остаток и делать выводы. 3^3 делится на 7 с остатком 6, 3^4 делится на 7 с остатком 4, 3^5 делится на 7 с остатком 5, 3^6 делится на 7 с остатком 1, 3^7 делится на 7 с остатком 3. Получили один из предыдущих остатков, значит «зациклились». Число 3^7 дает тот же остаток деления на 7, что и 3^1. Значит, длина цикла равна 6. $1989 = 331 \cdot 6 + 3$. Число 3^{1989} дает тот же остаток от деления на 7, что и 3^3, т. е. 6.

Контрольные вопросы

1. Сформулируйте алгоритм Евклида нахождения наибольшего общего делителя целых чисел.
2. Что значит расширенный алгоритм Евклида?
3. Какие числа называются взаимно простыми?
4. Объясните малую теорему Ферма.

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).
2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).
3. Условие задания.
4. Исполнительская часть.
5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

Числа для заданий даны в таблице.

1. Найдите канонические разложения чисел a и b.

2. Найдите НОД (a, b) пользуясь:

а) алгоритмом Евклида;

б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найдите целые u, v, удовлетворяющие соотношению Безу: $au + bv = $ НОД(a, b).

4. Найдите остаток от деления данного числа на простое.

Номер варианта	Задание
1	1–3. $a = 101398751$, $b = 326147777$. 4. Найти остаток от деления 1998^{2001} на 29
2	1–3. $a = 5999801$, $b = 48685811$. 4. Найти остаток от деления 2005^{2003} на 17
3	1–3. $a = 660422941$, $b = 36481301$. 4. Найти остаток от деления 2001^{2005} на 17
4	1–3. $a = 9002242397$, $b = 433817903$. 4. Найти остаток от деления 2004^{2998} на 19
5	1–3. $a = 9118515943$, $b = 3386496689$. 4. Найти остаток от деления 1999^{2005} на 23
6	1–3. $a = 5336161097$, $b = 196210799$. 4. Найти остаток от деления 1998^{2001} на 19
7	1–3. $a = 7049964661$, $b = 168687989$. 4. Найти остаток от деления 1997^{2004} на 17
8	1–3. $a = 83748733$, $b = 73435591$. 4. Найти остаток от деления 1996^{2003} на 11
9	1–3. $a = 16254559$, $b = 1029073$. 4. Найти остаток от деления 2006^{1998} на 19
10	1–3. $a = 6099377$, $b = 9568217$. 4. Найти остаток от деления 2006^{1999} на 17
11	1–3. $a = 7957549$, $b = 23118553$. 4. Найти остаток от деления 2005^{1999} на 19
12	1–3. $a = 16088437$, $b = 18216949$. 4. Найти остаток от деления 1995^{2004} на 16
13	1–3. $a = 244604911$, $b = 61875907$. 4. Найти остаток от деления 2001^{1995} на 17
14	1–3. $a = 356216713$, $b = 31238065$. 4. Найти остаток от деления 2005^{2004} на 19
15	1–3. $a = 7409621$, $b = 6793883$. 4. Найти остаток от деления 2005^{2002} на 29

Практическое занятие № 9

АВТОРСКОЕ ПРАВО И СМЕЖНЫЕ ПРАВА

Цель: изучить основные положения авторского права и смежных прав.

Теоретические сведения

Принципы и условия возникновения, реализации и защиты авторских и смежных прав. В качестве основных задач авторского права чаще всего в юридической литературе называются две следующие задачи. С одной стороны, авторское право должно стимулировать деятельность по созданию произведений науки, литературы и искусства. В этих целях авторское право способствует созданию условий для занятия творческим трудом; обеспечивает правовое признание и охрану достигнутых творческих результатов, закрепление за авторами прав на использование созданных ими произведений и получение доходов и т. д. С другой стороны, задачей авторского права считается создание условий для широкого использования произведений в интересах общества. Иными словами, повышение уровня охраны прав авторов ни в коем случае не должно препятствовать использованию их произведений в целях образования и просвещения или служить помехой в стремлении самой широкой аудитории читателей, зрителей, слушателей знакомиться с ними.

Указанные задачи авторского права тесным образом связаны с его принципами. Принципы авторского права – его основные начала, отправные идеи, которые обладают универсальностью, высшей императивностью и общезначимостью. Они пронизывают содержание всей системы авторского права, предопределяют всю юрисдикционную деятельность и воплощаются в субъективных правах и обязанностях участников авторских правоотношений. Не будучи закрепленными в конкретных статьях закона, принципы авторского права выводятся из анализа всей совокупности авторско-правовых норм. Знание принципов позволяет ориентироваться в обширном авторском законодательстве, правильно толковать

и применять на практике отдельные его нормы, а также решать вопросы, на которые нет прямого ответа в действующем законодательстве.

К числу основных принципов авторского права, отраженных в содержании его норм на современном этапе развития, относятся следующие.

Во-первых, принципом авторского права может и должен считаться принцип свободы творчества. Данный принцип, лишь недавно наполненный реальным содержанием, пронизывает собой все авторское законодательство и конкретизируется в целом ряде его норм.

Обеспечивая свободу творчества, авторское право охраняет все произведения науки, литературы и искусства независимо от их назначения, достоинств и способа выражения. В этих же целях закон не ограничивает круг охраняемых произведений каким-либо перечнем и охраняет любые результаты творческой деятельности, существующие в объективной форме. Творцы произведений свободны в выборе темы, сюжета, жанра и формы воплощения создаваемых ими художественных образов, а также самостоятельно решают вопросы о выпуске своего произведения в свет, придании произведению окончательной формы и т. п.

Во-вторых, принципом авторского права является сочетание личных интересов автора с интересами общества. Хотя данный принцип, безусловно, проявляется и в других институтах права интеллектуальной собственности и гражданского права в целом, в авторском праве он имеет особое значение. В основе авторского права лежит признанное за автором монопольное право на использование созданного им произведения. Определение разумных границ этой монополии на протяжении веков являлось одной из главных проблем авторского права. В настоящее время уже никто не утверждает, что авторы должны иметь неограниченный контроль за использованием своих произведений. Ничем не ограниченная монополия необходима и возможна лишь в отношении необнародованных произведений. Если же произведение с согласия автора стало доступно для всеобщего сведения, его права на произведение не могут быть столь обширными, чтобы полностью игнорировать интересы других граждан и общества в целом. Законы демократического общества не только гарантируют охрану интеллектуальной

собственности, но и закрепляют право членов общества на участие в культурной жизни и пользование достижениями культуры.

В-третьих, в качестве одного из принципов авторского права может быть выдвинуто положение о неотчуждаемости личных неимущественных прав автора. В этом состоит одно из существенных отличий отечественного авторского права от авторского права ряда зарубежных стран. По авторскому законодательству, личные неимущественные права автора (право на авторство, право на имя и пр.) не могут перейти к другим лицам, хотя бы сам автор и выразил на это свое согласие. Подобное соглашение не будет иметь юридической силы и является недействительным. Поэтому даже в тех случаях, когда произведение создано в порядке выполнения служебного задания, личные неимущественные права сохраняются за автором и должны быть во всех случаях обеспечены. Этими же соображениями продиктованы нормы законодательства, устанавливающие, что право авторства, право на авторское имя, право на защиту репутации автора не переходят по наследству, что в случаях так называемого «свободного» использования произведений обязательно указание имени автора и т. д. Что же касается имущественных прав авторов, то они могут передаваться другим лицам по авторскому договору, в порядке наследования, а также в силу закона (служебные произведения).

В-четвертых, для современного авторского права характерен принцип свободы авторского договора. Данный принцип заменил собой присущий ранее действующему авторскому праву принцип нормативной регламентации основных прав и обязанностей сторон по авторским договорам. Наиболее ярким выражением последнего было существование так называемых типовых авторских договоров (издательских, сценарных, постановочных и др.), которые имели нормативное значение и подробно регламентировали отношения авторов и пользователей произведений. Конечно, было бы неверно сводить роль типовых договоров лишь к ограничению свободы сторон в распоряжении принадлежащими им правами. Одной из главных функций типовых договоров было ограждение авторов от произвола пользователей произведений, стремление гарантировать авторам определенный минимальный уровень прав. Условия конкретных авторских договоров, ухудшающие положение авторов по сравнению с типовым договором, признавались недействительными и заменялись условиями, закрепленными в типовом договоре.

Вместе с тем присутствие в законодательстве правил, детально регулирующих сферу отношений, которая в принципе должна определяться прежде всего свободным волеизъявлением самих сторон, трудно признать нормальным явлением. В этой связи новое российское и белорусское авторские законодательства отказались от жесткой регламентации отношений сторон авторского договора. В нем закрепляются лишь возможные типы авторских договоров, а также указываются условия, которые должны быть в обязательном порядке согласованы сторонами. Что касается законных интересов авторов, то они обеспечиваются, с одной стороны, запретом включать в авторские договоры явно кабальные для авторов условия, например, условие о передаче прав на произведения, которые автор может создать в будущем, и, с другой стороны, правилами, предоставляющими авторам определенные права, например, на расторжение авторского договора по истечении пяти лет с даты его заключения, если конкретный срок договора не определен, или налагающими на пользователей произведений определенные обязанности, например, по выплате автору аванса по договору заказа. Кроме этих и других указанных в законе ограничений, стороны свободны в определении содержания авторского договора.

Интеллектуальная деятельность – это умственная (мыслительная, духовная, творческая) деятельность человека в области науки, техники, литературы, искусства и художественного конструирования (дизайна).

Признаки интеллектуальной деятельности:

1) интеллектуальная деятельность носит идеальный характер;

2) результатом интеллектуальной деятельности является выраженный в объективной форме ее продукт, именуемый в зависимости от его характера произведением науки, литературы, искусства, изобретением или промышленным образцом;

3) результаты интеллектуальной деятельности в отличие от объектов вещных прав имеют идеальную природу;

4) продуктом интеллектуальной деятельности могут быть средства индивидуализации юридического лица или индивидуального предпринимателя, а также индивидуализации выполняемых работ или услуг (фирменные наименования, товарные знаки, знаки обслуживания и наименования мест происхождения товаров).

Объект интеллектуальной собственности – это материализованный результат нематериального по своей природе мыслительного процесса.

К объектам интеллектуальной собственности в Республике Беларусь относятся:

1) результаты интеллектуальной деятельности:

– объекты авторского права и смежных прав;

– объекты патентного права;

2) средства индивидуализации участников гражданского оборота, товаров, работ или услуг;

3) другие результаты интеллектуальной деятельности и средства индивидуализации участников гражданского оборота, товаров, работ или услуг в случаях, предусмотренных Гражданским кодексом Республики Беларусь и иными законодательными актами.

Интеллектуальную собственность делят на две составляющие:

1) промышленную собственность;

2) авторское право.

К промышленной собственности относятся промышленные образцы, изобретения, полезные модели, товарные знаки, знаки обслуживания и фирменные наименования.

Объекты авторского права – это произведения искусства, литературные и музыкальные произведения, творения кинематографии, а также научные произведения.

Законодательство Республики Беларусь об авторском праве и смежных правах основывается на Конституции Республики Беларусь и состоит из Гражданского кодекса Республики Беларусь, Закона Республики Беларусь «Об авторском праве и смежных правах», нормативных правовых актов Президента и Правительства Республики Беларусь, других актов законодательства Республики Беларусь.

Основные положения авторского права. Авторское право распространяется на произведения науки, литературы и искусства, существующие в какой-либо объективной форме. Оно возникает в силу факта их создания. Для возникновения и осуществления авторского права не требуется соблюдения каких-либо формальностей.

Субъектами авторского права являются авторы (соавторы), наследники и иные правопреемники.

Первичными субъектами авторского права являются авторы произведений. Автор – физическое лицо, творческим трудом которого создано произведение. Если произведение создано совместным творческим трудом двух или более лиц, они признаются соавторами. При отсутствии доказательств иного автором произведения

считается лицо, указанное в качестве автора на оригинале или экземпляре произведения (презумпция авторства).

По закону субъектами авторского права в части имущественных прав, кроме авторов произведений, могут быть:

– наследники авторов;

– наниматели авторов служебных произведений;

– юридические лица и физические лица, заключившие с авторами и их наследниками договоры на использование произведений науки, литературы и искусства;

– правопреемники юридических и физических лиц;

– организации, управляющие имущественными правами авторов на коллективной основе.

Классификация объектов авторского права. Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме:

– письменной (рукопись, машинопись, нотная запись и др.);

– устной (публичное произнесение, публичное исполнение и др.);

– звуко- или видеозаписи (механическая, магнитная, цифровая, оптическая и др.);

– изображения (рисунок, эскиз, картина, карта, план, чертеж, кино-, теле-, видео-, фотокадр и др.);

– объемно-пространственной (скульптура, модель, макет, сооружение и др.);

– электронной, в том числе цифровой.

Объекты авторского права:

– литературные произведения;

– драматические и музыкально-драматические произведения, произведения хореографии и пантомимы и другие сценарные произведения;

– музыкальные произведения с текстом и без текста;

– аудиовизуальные произведения;

– произведения изобразительного искусства;

– произведения прикладного искусства и дизайна;

– произведения архитектуры, градостроительства и садово-паркового искусства;

– фотографические произведения, в том числе произведения, полученные способами, аналогичными фотографии;

– карты, планы, эскизы, иллюстрации и пластические произведения, относящиеся к географии, картографии и другим наукам;

– компьютерные программы (прикладные программы и операционные системы на любом языке и в любой форме, включая исходный текст и объектный код; базы данных или компиляции иных материалов в любой форме, представляющие собой по подбору и расположению материалов результат интеллектуального творчества);

– произведения науки;

– производные произведения (переводы, обработки, инсценировки, музыкальные аранжировки, обзор, аннотации, рефераты; сборники произведений: энциклопедии, антологии, атласы и другие составные произведения как результат творческого труда);

– составные произведения – сборники.

Не являются объектами авторского права:

– официальные документы (правовые акты, судебные постановления, иные документы административного и судебного характера, учредительные документы организаций), а также их официальные переводы;

– государственные символы и знаки (флаг, герб, гимн, государственные награды, денежные и иные знаки, почтовые марки);

– произведения народного творчества, авторы которых не известны.

Авторское право не распространяется на собственно идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты, даже если они выражены, отображены, объяснены или воплощены в произведении.

Общие положения относятся равным образом и к авторским, и к смежным правам. Они регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), постановок, исполнений, фонограмм, передач организаций эфирного и кабельного вещания (смежные права).

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

Источниками регулирования авторского права являются как законы Республики Беларусь, так и международные договоры.

Если последними установлены иные правила, чем те, которые содержатся в законе, то применяются правила международного договора.

Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено.

Передача права собственности на материальный объект или право владения материальным объектом само по себе не влечет передачи каких-либо авторских прав на произведение, выраженное в этом объекте.

Авторские права делятся на личные неимущественные (моральные права – droit moral) и имущественные (экономические) права (рис. 21).

Личные неимущественные права:

– признаваться автором произведения (право авторства);

– использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т. е. анонимно (право на имя);

– обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;

– право на защиту произведения, включая его название, от всякого рода искажений или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

Личное неимущественное право принадлежат автору независимо от его имущественных прав и сохраняется за ним даже после уступки исключительных прав на использование произведения.

Имущественные права – исключительное право осуществлять или разрешать осуществлять следующие действия:

– воспроизведение произведения;

– распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;

– прокат оригиналов или экземпляров компьютерных программ, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;

– импорт экземпляров произведения;

– публичный показ оригинала или экземпляра произведения;

– публичное исполнение произведения;

– передачу произведения в эфир;
– иное сообщение произведения для всеобщего сведения;
– перевод произведения на другой язык;
– переделку или иную переработку произведения.

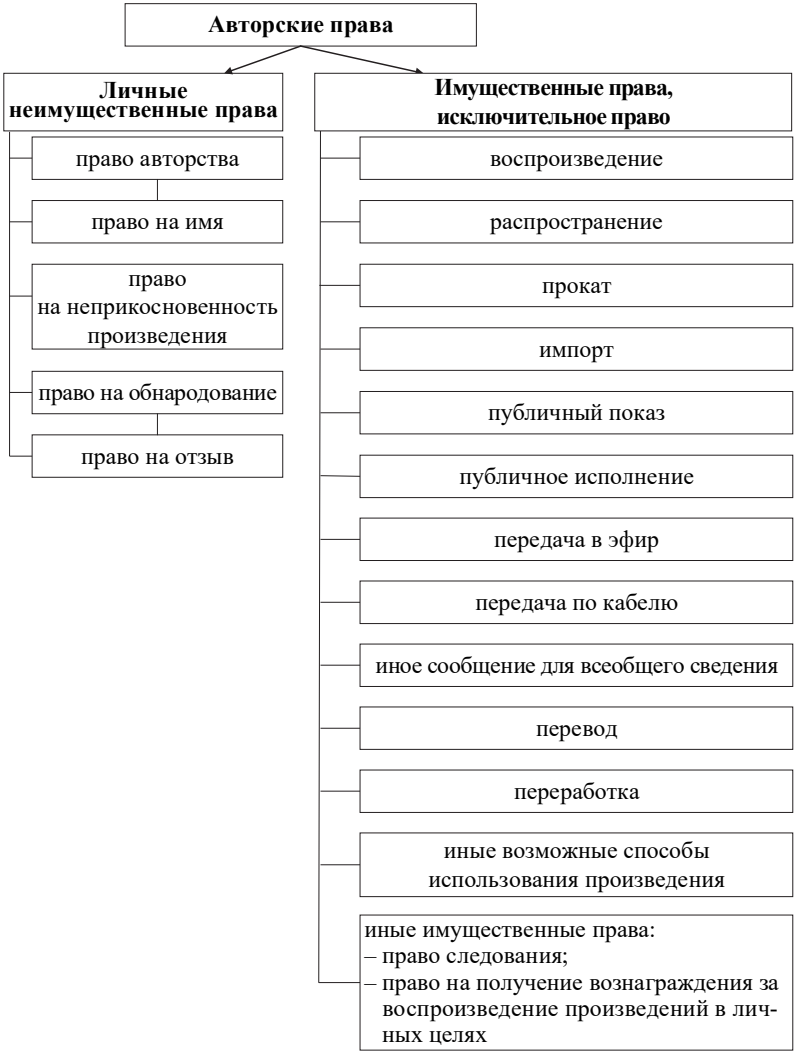

Рис. 21. Классификация авторского права

Автор принятого архитектурного проекта вправе требовать от заказчика предоставления права на участие в реализации своего проекта при разработке документации для строительства и при строительстве здания или сооружения.

Автор имеет право на авторское вознаграждение за каждый вид использования произведения.

Авторское право на произведение науки, литературы и искусства возникает в силу факта его создания и не требует регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Авторское право на составные произведения:

– автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и распоряжение материалов как результат творческого труда (составительство);

– составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное;

– авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором;

– авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений;

– лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания;

– авторы произведений, включенных в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания в целом, если иное не предусмотрено авторским договором.

Авторское право на производные произведения:

– переводчикам и авторам других производных произведении принадлежит авторское право на осуществленные ими перевод, инсценировку, аранжировку или другую переработку при условии соблюдения ими прав автора произведения;

– авторское право переводчика и авторов других производных произведений не препятствует иным лицам осуществлять свои переводы и переработки тех же произведений.

Авторское право на аудиовизуальные произведении:

– авторами аудиовизуального произведения являются режиссер-постановщик, автор сценария, автор специально созданного для аудиовизуального произведения музыкального произведения с текстом или без текста;

– заключение договора на создание аудиовизуального произведения влечет за собой передачу авторами этого произведения производителю исключительных прав на воспроизведение, распространение, публичное исполнение, сообщение для всеобщего сведения, а также субтитрирование и дублирование текста, если иное не предусмотрено договором. Указанные права действуют в течение срока действия авторского права на аудиовизуальное произведение. Производитель аудиовизуального произведения вправе при любом использовании этого произведения указывать свое имя или наименование либо требовать такого указания;

– автор музыкального произведения с текстом или без текста сохраняет право на вознаграждение за публичное исполнение его музыкального произведения при использовании аудиовизуального произведения, включающего данное музыкальное произведение;

– авторы ранее существовавших произведений, включенных в аудиовизуальное произведение или переработанных для него, сохраняют авторское право на свои произведения и могут использовать их отдельно от аудиовизуального произведения.

Ограничения имущественных прав:

1) воспроизведение произведения в личных целях исключительно физическим лицом в единичных экземплярах;

2) не распространяется на воспроизведение: произведений архитектуры в форме зданий или других сооружений; баз данных или существенных частей из них; компьютерных программ, нотных текстов и книг (полностью) посредством репродуцирования;

3) использование произведения без согласия автора и без выплаты авторского вознаграждения с обязательным указанием автора произведения и источника заимствования;

4) цитирование в научных, исследовательских, учебных, полемических, критических и информационных целях отрывков, использование их в качестве иллюстраций в изданиях, радио- и телепередачах,

звуко- и видеозаписях учебного характера, воспроизведение в газетах и т. п.;

5) репродуцирование произведений библиотеками, архивами и образовательными учреждениями с обязательным указанием автора произведения и источника заимствования в единичном экземпляре без извлечения прибыли;

6) воспроизведение компьютерных программ только для архивных целей или для замены правомерно приобретенного экземпляра, для обеспечения совместной работы с другими программами без использования для создания других компьютерных программ, аналогичных адаптируемой.

Срок действия авторского права. Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

Общественное достояние по истечении срока действия имущественных прав на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние, т. е. они могут свободно использоваться любым физическим или юридическим лицом без выплаты вознаграждения.

Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора действует без ограничения срока.

Автор вправе указать лицо, на которое он возлагает охрану своих личных неимущественных прав после своей смерти и которое осуществляет свои полномочия пожизненно. При отсутствии указаний охрана осуществляется его наследниками или специально уполномоченным государственным органом Республики Беларусь при отсутствии наследников.

Служебные объекты авторского права. Личные неимущественные права на произведение, созданное в порядке выполнения служебного задания или служебных обязанностей (служебное произведение), принадлежат автору.

Исключительные права на использование служебного произведения принадлежат лицу, с которым автор состоит в трудовых отношениях (работодателю), если в договоре между ними не предусмотрено иное.

Автор служебного произведения не вправе препятствовать его обнародованию нанимателем.

Сформулировано положение, призванное согласовать интересы авторов и работодателей. Прежде всего, подтвержден принцип принадлежности автору авторского права на произведение, созданное в порядке выполнения служебных обязанностей или служебного задания работодателя. Вместе с тем введена презумпция принадлежности работодателю исключительных прав на использование служебного произведения, если в договоре между ним и автором не предусмотрено иное. Одновременно сняты все ограничения на выплату вознаграждения автору за использование служебного произведения и подчеркнуто, что размер авторского вознаграждения за каждый вид использования служебного произведения и порядок его выплаты устанавливаются договором между автором и работодателем, а также в договорах, заключаемых организациями, управляющими правами авторов на коллективной основе, с пользователями.

Субъекты авторского права и смежных прав. Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства. Им может быть и гражданин, не достигший восемнадцатилетнего возраста, и душевнобольной. Так, авторские права детей, представленные на смотры или выставки детской или юношеской самодеятельности и т. д., защищаются авторским правом.

Но недееспособные, став субъектами авторского права, не имеют права самостоятельно совершать какие-либо сделки, связанные с использованием авторского права. Несовершеннолетние в возрасте от 14 до 18 лет могут самостоятельно осуществлять авторские права на свои произведения.

За авторами – гражданами Республики Беларусь и их правопреемниками авторское право признается на все произведения независимо от места их обнародования или нахождения в какой-либо объективной форме.

Если произведение обнародовано либо не обнародовано, но существует на территории Республики Беларусь в какой-либо объективной форме, то авторское право распространяется на такое произведение независимо от гражданства автора.

За гражданами других государств, обнародовавшими свои произведения за пределами Республики Беларусь, авторское право признается в соответствии с международными договорами Республики Беларусь.

Лицо, обозначенное в качестве автора на оригинале или экземпляре произведения, считается его автором, если отсутствует доказательство иного.

При обнародовании произведения анонимно или под псевдонимом (за исключением случаев, когда псевдоним автора не вызывает сомнения в его личности), издатель, имя или наименование которого обозначено на произведении, при отсутствии доказательств иного, считается представителем автора и имеет право защищать права автора и обеспечивать их осуществление. Это положение действует до тех пор, пока автор не раскроет свою личность и не заявит о своем авторстве.

Соавторство всегда является результатом соглашения о совместной работе. По крайней мере, между соавторами должно быть хотя бы устное или подразумеваемое соглашение о создании коллективного произведения.

Недействительным является соавторство, навязанное автору лицом, от которого так или иначе зависит использование произведения.

Оказание автору технической помощи соавтора не порождает. При соавторстве должно быть творческое участие лиц в создании произведения.

В юридической литературе выделяют два вида соавторства: нераздельное и раздельное.

Нераздельное соавторство возникает в отношении произведения, составляющего одно неразрывное целое. При нераздельном соавторстве выделить долю каждого автора в произведении невозможно, поэтому все соавторы пользуются неделимым авторским правом на все произведение в целом и на каждую его часть.

Раздельное соавторство возникает на одно произведение, каждая часть которого выполнена самостоятельным автором, и долю каждого из них можно легко установить (соавторство композитора и либреттиста, соавторство на учебник группы авторов и т. д.). В этом случае наряду с совместным и неделимым правом всех соавторов на произведение в целом каждый из авторов сохраняет свое право на созданную им часть произведения, имеющую самостоятельное значение. Например, можно требовать указания своего авторства в отношении этой части и самостоятельно распоряжаться ее использованием, поскольку такое осуществление возможно отдельно от других частей, если иное не предусмотрено соглашением между соавторами.

Отношения между соавторами могут быть определены их соглашением. При отсутствии такого соглашения авторское право на коллективное произведение осуществляется всеми соавторами совместно. Споры между соавторами разрешаются судом.

Субъектами авторского права после смерти автора становятся наследники. Наследование авторских прав может происходить как по закону, так и по завещанию.

Особенности наследования авторских прав следующие.

Прежде всего, по наследству к наследникам переходят не все авторские права, а только их часть. В законе указывается, что по наследству не переходят право авторства, право на авторское имя и право на защиту репутации автора.

Однако и в отношении этих прав к наследникам переходят права на защиту названных прав от нарушений со стороны третьих лиц, если только автор не назначил для этих целей специальное лицо.

В отличие от прав на произведения самих авторов, которые носят пожизненный характер, авторские права наследников ограничены установленным законом сроком. Авторские права наследников действуют в течение 50 лет после смерти автора, считая с 1 января года, следующего за годом смерти.

Из этого общего правила есть ряд исключений:

а) если произведение создано в соавторстве, то 50-летний срок исчисляется после смерти последнего из соавторов;

б) если произведение впервые выпущено в свет после смерти автора, то авторское право действует в течение 50 лет после выпуска его в свет;

в) если автор был репрессирован и реабилитирован посмертно, то произведение охраняется 50 лет после реабилитации;

г) если автор воевал или работал во время Великой Отечественной войны, то срок охраны увеличивается на четыре года, и т. д.

Важной особенностью наследования авторских прав является то, что авторские права переходят к наследнику в бездолевом порядке, как единое целое, не подлежащее ни выделу, ни разделу. Это означает, что распоряжаться перешедшими по наследству авторскими правами наследники должны совместно и по взаимному согласию, а в случае спора – по решению суда.

Помимо наследников авторские права могут переходить к иным правопреемникам. В их роли выступают издательства,

театры, киностудии и другие организации, занимающиеся использованием произведений. Они приобретают авторские права на основании заключенных с авторами и наследниками авторских договоров.

Становясь обладателями авторских прав, эти организации используют произведения и распоряжаются ими такими способами, которые предусмотрены конкретными авторскими договорами, и в установленных ими пределах.

Субъекты смежных прав: исполнители, производители фонограмм, организации эфирного или кабельного вещания.

Сфера действия смежных прав: исполнители граждане и не граждане Республики Беларусь, исполнения которых имеют место на территории Республики Беларусь, или включены в фонограммы, или не записаны на стенограмму, но содержатся в передачах организаций эфирного или кабельного вещания, охраняемые в соответствии с законом.

Права исполнителя: на имя; на защиту репутации; на использование исполнения в любой форме, включая право на получение вознаграждения за каждый вид использования исполнения.

Исключительное право на использование: передавать в эфир или сообщать для всеобщего сведения по кабелю исполнение; записывать ранее не записанное исполнение; воспроизводить запись исполнения; передавать в эфир или по кабелю запись исполнения; распространять оригинал или экземпляры исполнения, записанного на фонограмму; сдавать в прокат оригинал или экземпляры записанного на фонограмму исполнения; сообщать для всеобщего сведения исполнение, записанное на фонограмму, по проводам или средствами беспроволочной связи.

Права производителя фонограммы: на использование ее в любой форме, включая право на получение вознаграждения за каждый вид использования фонограммы: воспроизводство; переработку; распространение; импортирование; сдача в прокат; доведение до всеобщего сведения.

Использование фонограммы, опубликованной в коммерческих целях: публичное исполнение фонограммы; передача фонограммы в эфир; иное сообщение фонограммы для всеобщего сведения.

Допускается воспроизведение фонограмм: для включения в обзор о текущих событиях отрывков из исполнения, фонограммы,

передачи организации эфирного или кабельного вещания; исключительно в целях обучения или научного исследования; для цитирования в форме отрывков из исполнения.

Коллективное управление имущественными правами обладателей авторского права и смежных прав в случаях, когда их трудно практически осуществить в индивидуальном порядке, могут осуществлять организации, порядок создания и деятельности которых определяется законодательством Республики Беларусь.

Защита и охрана авторских прав в Республики Беларусь и за рубежом. Под защитой авторских прав понимается совокупность мер, направленных на восстановление и признание этих прав при их нарушении или оспаривании. Действующее законодательство содержит достаточно подробную регламентацию видов, форм, средств и способов защиты авторских прав.

Защита авторских прав может осуществляться уголовно-правовым, административно-правовым и гражданско-правовым способом.

Наиболее опасные посягательства на субъективные авторские права рассматриваются как преступления и влекут за собой уголовную ответственность: за незаконное использование объектов авторского права, а равно присвоение авторства, если эти деяния причинили крупный ущерб; за те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой.

Административно-правовой способ защиты авторских прав состоит в рассмотрении жалоб авторов и других заинтересованных лиц, а также протестов прокуроров организациям, вышестоящим по отношению к организациям, использующим произведения авторов – министерствам, государственным комитетам и т. д. Эти организации осуществляют защиту прав авторов и по собственной инициативе в случаях обнаружения фактов их нарушения.

Защита авторских прав осуществляется Комитетом по авторским правам Министерства образования и авторскими союзами.

Преобладающим является гражданско-правовой способ защиты.

Защита личных неимущественных прав автора осуществляется вне зависимости от вины их нарушителя и независимо от нарушения имущественных интересов автора. Исковая давность

по спорам о нарушении личных неимущественных прав не применяется.

Требования об устранении допущенных нарушений личных неимущественных прав могут быть предъявлены автором, а после его смерти – наследниками или лицом, на которое автор возложил охрану неприкосновенности своих произведений, а также организациями, на которые возложена охрана авторских прав.

Закон Республики Беларусь «Об авторском праве и смежных права» определяет ряд мер, которые могут быть применены в целях защиты нарушенных авторских прав. Так, в соответствии с этим законом суд может вынести определение о запрете осуществляемой ответчиком противоправной деятельности, к которой относится изготовление, воспроизведение, продажа, импорт или иное предусмотренное законом использование, а также транспортировку, хранение или владение с целью выпуска в гражданский оборот экземпляров произведения и фонограмм, в отношении которых предполагается, что они являются контрафактными. (Контрафактными являются экземпляры произведения или фонограммы, изготовление или распространение которых влечет за собой нарушение авторских и смежных прав.)

Обладатели исключительных авторских прав вправе требовать от нарушителя: признания прав; восстановления положения, существовавшего до нарушения права. Восстановление нарушенного права может состоять во внесении соответствующего исправления в произведение, в его заглавие или титульный лист, указании имени автора и т. д. Если исправить нарушение таким образом невозможно, то автор может требовать публикации в печати о допущенных нарушениях; пресечения действий, нарушающих право или создающих угрозу его нарушения; возмещения убытков, включая упущенную выгоду. Под убытками в этом случае понимаются как понесенные кредитором расходы, так и не полученные им по вине должника доходы.

Расходы автора могут состоять, например, в затратах на устранение искажений в его произведении.

Неполученные доходы (упущенная выгода) – это вознаграждение, которое автор получил бы при отсутствии нарушений его авторских прав.

Размер убытков определяется с учетом качества произведения и ставок вознаграждения, предусмотренных для аналогичных произведений или способов их использования.

Требования о возмещении убытков могут быть предъявлены независимо от требований по защите личных неимущественных прав автора, но удовлетворены лишь в пределах срока исковой давности; взыскания дохода, полученного нарушителем вследствие нарушения авторских прав, вместо возмещения убытков; выплаты компенсации, определяемой по усмотрению суда, вместо возмещения убытков или взыскания дохода; принятия иных предусмотренных законодательными актами мер, связанных с защитой их прав. В частности, автор может предъявить иск с требованием признать, что он не является автором приписываемого ему произведения.

За защитой своего права обладатель исключительных авторских прав может обратиться в установленном порядке в судебные органы в соответствии с их компетенцией.

Суд выносит решение о конфискации контрафактных экземпляров произведения или фонограммы, а также материалов и оборудования, используемых для их воспроизведения.

По требованию обладателя авторских прав контрафактные экземпляры и фонограммы могут быть ему переданы. Если такого требования нет, контрафактные экземпляры произведения подлежат уничтожению.

Управление имущественными правами авторов и обладателей смежных прав на коллективной основе. В случаях, когда управление имущественными правами авторов и обладателей смежных прав трудно практически осуществить в индивидуальном порядке, для обеспечения имущественных прав авторов, исполнителей, производителей фонограмм и иных обладателей авторского права и смежных прав могут создаваться организации, осуществляющие и охраняющие права указанных лиц на коллективной основе.

Порядок создания и деятельности таких организаций определяется законодательством Республики Беларусь. Это право закреплено в законе Республики Беларусь «Об авторском праве и смежных правах», ст. 42 «Коллективное управление имущественными правами».

Контрольные вопросы

1. На какие объекты распространяется авторское право?
2. Что относится к личным неимущественным правам?
3. Что относится к личным имущественным правам?
4. Каковы особенности авторского права на составные произведения?
5. Каков срок действия авторского права?
6. Кто является субъектом авторского права?

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).
2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).
3. Ответы на вопросы.
4. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Практическое занятие № 10

ПАТЕНТНЫЙ ПОИСК

Цель: изучить виды, содержание и порядок проведения патентных исследований.

Теоретические сведения

Целью патентных исследований является определение уровня техники, который используется для проверки соответствия заявленного изобретения условиям патентоспособности «новизна» и «изобретательский уровень».

Патентное исследование проводится на основании формулы изобретения с учетом описания и чертежей, если они имеются, а также с учетом изменений формулы изобретения, принятых во внимание при рассмотрении заявки.

При определении уровня техники общедоступными считаются сведения, содержащиеся в источниках информации, с которыми любое лицо может ознакомиться само либо о содержании которых ему может быть законным путем сообщено.

Ниже представлен перечень источников для поиска патентной информации:

– Национальный центр интеллектуальной собственности (https://bypatents.com/);

– Российское агентство по патентам и товарным знакам (Роспатент) (www.rospatent.gov.ru);

– Федеральный институт промышленной собственности (http://www.fips.ru);

– Евразийское патентное ведомство (http://www.eapo.org);

– бесплатный поиск по патентам США на сайте компании United States Patent and Trademark Office (http://www.uspto.gov);

– Европейский патентный офис (http://www.epo.org);

– Патентное бюро Японии (www.jpo.go.jp).

Международные классификаторы. Для обеспечения единообразия в международном масштабе распределения патентных документов, а также упрощения поиска необходимой патентной

документации применяются специально разработанные патентные классификаторы.

Международная патентная классификация (МПК), принятая в соответствии со Страсбургским соглашением 1971 г., предусматривает создание единой системы классификации, охватывающей патенты на изобретения, включая опубликованные патентные заявки, авторские свидетельства, полезные модели и свидетельства о полезности. Аббревиатура «МПК» является общепринятым обозначением Международной патентной классификации.

Международная классификация промышленных образцов (МКПО) была принята 8 октября 1968 г. дипломатической конференцией в г. Локарно (Швейцария), на которую были приглашены все страны – участницы Парижской конвенции по охране промышленной собственности.

Международная классификация товаров и услуг (МКТУ) в соответствии с Ниццким соглашением от 15 июня 1957 г., отражая единую классификацию товаров и услуг для регистрации товарного знака, позволяет с максимальной достоверностью идентифицировать и, соответственно, классифицировать товар или услугу с обеспечением их единообразного восприятия всеми заинтересованными лицами.

Универсальная десятичная классификация (УДК), первое сводное издание которой вышло в 1905 г. в Брюсселе, получила широкое применение в качестве единой системы классификации информационных материалов в области естественных и технических наук. Ее применение позволяет обеспечить единообразие в организации справочно-информационных фондов в органах научно-технической информации, научных и технических библиотеках страны.

Международная патентная классификация (МПК). МПК является средством для единообразного в международном масштабе классифицирования патентных документов, позволяет эффективно осуществлять поиск патентных документов с целью установления новизны и оценки вклада изобретателя в заявленное техническое решение (включая оценку технической прогрессивности и полезного результата). До 1 января 1990 г. использовалось обозначение МКИ – Международная классификация изобретений.

МПК, кроме того, является:

– инструментом для упорядоченного хранения патентных документов, что облегчает доступ к содержащейся в них технической и правовой информации;

– основой для избирательного распределения информации среди потребителей патентной информации;

– основой для определения уровня техники в отдельных областях;

– основой для получения статистических данных в области промышленной собственности, что в свою очередь позволит определять уровень развития различных отраслей техники.

МПК охватывает все области знаний, объекты которых могут подлежать защите охранными документами. Иерархическая структура МПК выражается в разбивке всех областей знаний на несколько классификационных уровней. В нисходящем порядке эти уровни иерархии соответствуют разделам, классам, подклассам, основным группам и подгруппам.

По своей структуре МПК разделена на восемь основных разделов.

Каждый раздел обозначен заглавной буквой латинского алфавита от A до H – это индекс раздела.

Заголовок раздела лишь приблизительно отражает его содержание. Разделы имеют следующие названия:

A – удовлетворение жизненных потребностей человека;

B – различные технологические процессы; транспортирование;

C – химия; металлургия;

D – текстиль; бумага;

E – строительство; горное дело;

F – механика; освещение; отопление; двигатели и насосы; оружие; боеприпасы; взрывные работы;

G – физика;

H – электричество.

В оглавлении к каждому разделу помещен перечень относящихся к нему классов и подклассов.

Внутри разделов родственные классы условно объединяются в подразделы, которые не обозначаются индексами.

Например, в разделе D имеются подразделы: натуральные и химические нити и волокна; прядение; пряжа; окончательная обработка пряжи; ткачество; плетение; изготовление кружев; трикотажно-вязальное производство; нетканые материалы; шитье, вышивание, производство прошивных изделий; обработка текстильных изделий,

стирка, эластичные материалы; канаты, тросы или кабели; производство бумаги; производство целлюлозы.

Каждый раздел делится на классы. Индекс класса состоит из индекса раздела и двузначного числа. Например: D 06

Заголовок класса отражает его содержание. Например: D 06 Обработка текстильных изделий; стирка; эластичные материалы, не отнесенные к другим классам.

Далее идет разбивка по подклассам, основным группам и подгруппам.

Полный классификационный индекс состоит из комбинации символов, используемых для обозначения раздела, класса, подкласса и основной группы или подгруппы.

Международная классификация промышленных образцов (МКПО). МКПО служит для классифицирования промышленных образцов и состоит из перечня классов и подклассов и алфавитного перечня наименований изделий, в котором промышленные образцы объединены с указанием соответствующих им классов и подклассов.

Например: Класс 02 – предметы одежды, галантерея.

Международная классификация товаров и услуг (МКТУ). МКТУ используется при регистрации товарных знаков либо в качестве основной (единственной), либо вспомогательной классификации. В официальных публикациях о регистрации знаков указываются номера классов МКТУ товаров/услуг, в отношении которых зарегистрированы знаки.

Заголовки классов указывают в общем виде только области, к которым товары и услуги в принципе могут относиться, и не содержат названия конкретных товаров или услуг.

Для правильной классификации каждого конкретного товара или услуги необходимо пользоваться непосредственно перечнями товаров и услуг и пояснениями к каждому классу.

Например: Класс 25 – Одежда, обувь, головные уборы.

Порядок выполнения работ по патентным исследованиям. В общем случае порядок выполнения работ по патентным исследованиям состоит из следующих этапов.

1. *Разработка регламента поиска*. Регламент поиска включает выбор источников информации страны, в которой будет вестись

поиск, его ретроспективу и указание источников (этот этап оформляется в виде табл. 9).

Таблица 9

Источники информации

Предмет поиска (объект исследования, его составные части	Страна поиска	Патентные		НТИ		Конъюнктурные		Другие		Ретроспективность	Наименование информационной базы (фонда)
		Наименование	Классификационные рубрики: МПК (МКИ), МКПО, МКТУ и др.	Наименование	Рубрики УДК и др.	Наименование	Код товара ГС, СМТК, БТН	Наименование	Классификационные индексы		
1	2	3	4	5	6	7	8	9	10	11	12

Основные сведения по структуре и применению международных классификаторов приводятся выше в тексте.

2. *Поиск и отбор патентной и другой научно-технической документации.* Поиск должен осуществляться при наименьших затратах времени и с помощью автоматизированных информационных систем. Поиск в зарубежном патентном ведомстве должен быть согласован с национальным патентным ведомством – Национальным центром интеллектуальной собственности. Материалы, отобранные для поиска, должны включать патентную документацию, научно-техническую, конъюнктурную, ТНПА (технические нормативно-правовые акты) и материалы государственной регистрации НИОКР (научно-исследовательские и опытно-конструкторские работы).

Данный этап оформляется в виде табл. 10 и 11.

3. *Систематизация и анализ отобранной документации.* По выявленным в процессе поиска документам, требующим, например, в случае нарушения прав объектов промышленной собственности незамедлительного принятия решений руководством организации, выводы и рекомендации исполнителей патентных исследований оформляются в виде экспертного заключения.

Таблица 10

Патентная документация

Предмет поиска (объект исследования, его составные части)	Страна выдачи, вид и номер охранного документа. Классификационный индекс	Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации	Название изобретения (полезной модели, промышленного образца)	Сведения о действии охранного документа или причина его аннулирования (только для анализа патентной чистоты)
1	2	3	4	5

Таблица 11

Научно-техническая, конъюнктурная документация, ТНПА и материалы государственной регистрации НИОКР

Предмет поиска (объект исследования, его составные части)	Наименование источника информации с указанием страницы источника, номера и даты госрегистрации для НИОКР	Автор, фирма (держатель) технической документации	Год, место и орган издания (утверждения, депонирования источника), дата и номер регистрации для НИОКР
1	2	3	4

В общем случае анализ отобранной документации включает:

– технический уровень и тенденции развития объекта;

– патентно-лицензионную ситуацию;

– использование объектов промышленной собственности и наличие у них правовой охраны;

– исследование патентной чистоты объекта.

4. *Оформление результатов исследований в виде отчета о патентных исследованиях.* Отчет о патентных исследованиях должен содержать:

– титульный лист;

– список исполнителей;

– содержание;

– перечень сокращений, условных обозначений, символов, единиц, терминов;

– общие данные об объекте исследования;

– основную (аналитическую) часть;

– заключение;

– приложения.

Каждый из разделов аналитической части (ее содержание определяет третий этап) должен включать:

– анализ и обобщение информации в соответствии с поставленными перед патентными исследованиями задачами;

– выводы и рекомендации для достижения конечного результата данной работы;

– оценку соответствия результатов патентных исследований заданию на их проведение, обоснование необходимости проведения дополнительных исследований.

В заключении в общем случае приводят:

– оценку состояния выполнения работы, составной частью которой являются патентные исследования, и ее соответствие планам программ, перспективным целям деятельности предприятия (организации);

– предложения по использованию результатов патентных исследований для создания новых объектов техники, замены или снятия с производства неконкурентоспособных объектов техники, приобретения лицензий, правовой охраны объектов промышленной собственности, получения доходов от продажи лицензий на объекты промышленной собственности или «ноу-хау».

Разделы аналитической части отчета иллюстрируются таблицами, например «Патентно-лицензионная ситуация» (табл. 12), «Исследование патентной чистоты объекта техники» (табл. 13).

Таблица 12

Патентно-лицензионная ситуация

Объект техники и его составные части	Страна подачи заявки	Количество патентов, опубликованных заявок по годам подачи заявки (исключая патенты-аналоги)				
1	2	3	4	5	6	7

Примечание. Количество граф определяется глубиной поиска.

Таблица 13

Исследование патентной чистоты объекта

Наименование объекта техники и его составных частей	Обозначение (чертежей, ГОСТ, ТУ и т. д.). Дата утверждения чертежа	Страна, в отношении которой производится исследование патентной чистоты	Источники известности		Действующие охранные документы (в том числе патенты, аналоги, выложенные и акцептованные заявки), подлежащие анализу	Необходимость проведения сопоставительного анализа с объектом промышленной собственности («Подлежит» – «Не подлежит»)	Примечание
			Необходимость проведения сопоставительного анализа с объектом промышленной собственности («Подлежит» – «Не подлежит»)	Патенты, выложенные и акцептованные заявки (номер документа, даты приоритета и публикации, название объекта промышленной собственности, другие библиографические данные)			
1	2	3	4	5	6	7	8

Контрольные вопросы

1. Что такое патентное исследование?
2. Что такое патентная чистота?
3. В чем заключается этап разработки регламента поиска?
4. Что включает в себя этап систематизации и анализа отобранной документации?
5. Как происходит оформление результатов исследований в виде отчета о патентных исследованиях?

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).
2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).
3. Условие задания.
4. Исполнительская часть.
5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

В результате проведения исследовательских и проектно-конструкторских работ на промышленных предприятиях были разработаны методы испытания материалов. Для реализации этих методов предложены конструктивные решения приборов и приспособлений. В результате модернизации и совершенствования технологических процессов были рассмотрены решения, позволяющие повысить качество и производительность выпускаемой продукции. Предполагается патентование разработок.

Необходимо выполнить экспертизу патентной чистоты разработанных конструктивных решений: методов испытания материалов и устройств для их осуществления; устройств и механизмов для реализации технологических процессов. Соответствие вариантов выданным рисункам представлено ниже.

Номер варианта	Название
1, 9, 17, 25	Интерактивная система сканирования, ввода и визуального отображения графических изображений
2, 10, 18, 26	Динамическая платформа для симуляторов виртуальной реальности
3, 11, 19, 27	Идентификационная карта и способ проверки личности пользователя
4, 12, 20, 28	Устройство для счета банкнот
5, 13, 21, 29	Интерактивная игровая система
6, 14, 22, 30	Способ определения расстояния до объекта посредством цифровой фотокамеры
7, 15, 23	Устройство пофрагментного сканирования графических документов
8,16, 24	Игровое устройство для симуляции вождения

Пример выполнения задания

Задание. В результате проведения исследовательских работ по обеспечению требований безопасности работающих на производстве было предложено конструктивное выполнение светозащитных очков, внешний вид которых представлен на рис. 22.

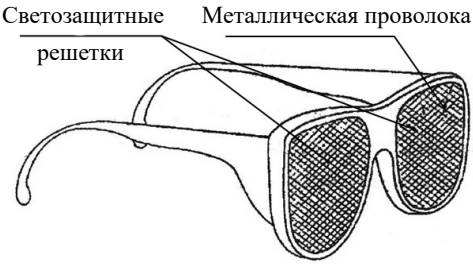

Рис. 22. Светозащитные очки

Наличие предполагаемых существенных признаков и планируемый выпуск продукции являются предпосылками для патентования разработки.

Необходимо выполнить экспертизу патентной чистоты разработанного конструктивного решения объекта промышленной собственности.

В качестве существенных признаков при патентовании предполагаемого изобретения выносится конструктивный признак: выполнение светозащитных решеток из металлических нитей.

Выполнение задания. Для выявления патентной чистоты разработанного объекта промышленной собственности следует использовать следующий регламент поиска:

– объект – очки с линзами, выполненными в виде сеток, ячеек;

– страна поиска – Республика Беларусь;

– источники информации – патентные;

– ретроспективность – 5 лет;

– информационная база – Афіцыйны бюлетэнь «Вынаходствы, карысныя мадэлі, прамысловыя узоры» Нацыянальнага цэнтра інтэлектуальнай уласнасці Рэспублікі Беларусь, каталог МПК (http://www.belgospatent.org.by).

Для проведения патентного поиска необходимо определить классификационную рубрику предполагаемого изобретения, которая в данном случае классифицируется по разделу «ФИЗИКА», класс «G02 Оптика».

Проведенный патентный поиск по указанному классу выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные на рис. 23–26.

Все данные по обнаруженным патентам-аналогам сводятся в соответствующую таблицу (табл. 14).

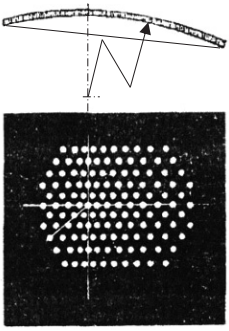

Рис. 23. Изобретение «Фильтр оптический перфорационный», патент 4097

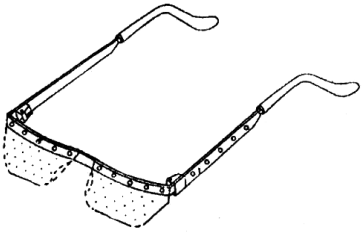

Рис. 24. Полезная модель «Универсальная очковая оправа открытого типа», патент 107U

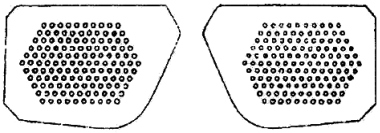

Рис. 25. Полезная модель «Сетчатый окуляр», патент 309U

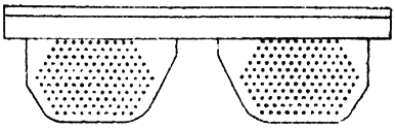

Рис. 26. Полезная модель «Сетчатые очки с защитой от электромагнитных и электростатических воздействий», патент 256U

Таблица 14

Патентная документация

Предмет поиска (объект исследования, его составные части)	Страна выдачи, вид и номер охранного документа. Классификационный индекс	Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации	Название изобретения (полезной модели, промышленного образца)	Сведения о действии охранного документа или причина его аннулирования
Сетчатые окуляры, светозащитные очки, защитные очки	Патент РБ № 4097 МПК G02C	Желтов Г. И., Ковшель Н. М. Заявка a19970332 от 18.06.1997, опубл. 30.09.2001 ОБ № 3, 2001	«Фильтр оптический перфорационный»	Действует

Окончание табл. 14

Предмет поиска (объект исследования, его составные части)	Страна выдачи, вид и номер охранного документа. Классификационный индекс	Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации	Название изобретения (полезной модели, промышленного образца)	Сведения о действии охранного документа или причина его аннулирования
Сетчатые окуляры, светозащитные очки, защитные очки	Патент РБ № 107U МПК G02C	Пешков А. Н., Пешков С. А. Заявка u19990022 от 11.03.1999, опубл. 30.03.2000 ОБ № 1, 2000	«Универсальная очковая оправа открытого типа»	Действует
	Патент РБ № 309U МПК G02C	Пешков А. Н., Пешков С. А. Заявка u20000101 от 15.06.2000, опубл. 30.03.2001 ОБ № 3, 2001	«Сетчатый окуляр»	Действует
	Патент РБ № 4097 МПК G02C	Пешков А. Н., Пешков С. А. Заявка u20000091 от 06.06.2000, опубл. 30.03.2001 ОБ № 3, 2001	«Сетчатые очки с защитой от электромагнитных и электростатических воздействий»	Действует

Дальнейший анализ содержания обнаруженной патентной информации, выполняемой специалистами, позволяет определить наличие существенных отличий и возможность получения патента на изобретение или полезную модель.

Практическое занятие № 11

НАСТРОЙКА АНТИВИРУСОВ

Цель: овладеть навыками настройки и использования различных антивирусов.

Теоретические сведения

Компьютерный вирус – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

Процесс внедрения вирусом своей копии в другую программу (системную область диска и т. д.) называется **заражением**, а объект, содержащий вирус (программа или иной), является **зараженным**.

Основными **путями** проникновения вирусов в компьютер являются съемные носители информации (**диски** и **флэш-карты**), а также **компьютерные сети**. Заражение жесткого диска вирусом может произойти при загрузке компьютера с диска, содержащего вирус. Такое заражение может быть и случайным, например, если флешку не вынули и перезагрузили компьютер. Заразить диск гораздо проще – вирус может попасть на нее, даже если флеш-карту просто вставили в зараженный компьютер и просмотрели ее содержимое. **Зараженный диск** – это диск, в загрузочном секторе которого находится вирус.

После запуска программы, содержащей вирус, становится возможным заражение других файлов. **Зараженный файл** – это файл, содержащий внедренный в него вирус.

Признаки появления вирусов в компьютере:

– уменьшение производительности работы компьютера;

– невозможность и замедление загрузки операционной системы;

– повышение числа файлов на диске;

– замена размеров файлов;

– периодическое появление на экране монитора неуместных сообщений;

– уменьшение объема свободной операционной системы;
– резкое возрастание времени доступа к жесткому диску;
– разрушение файловой структуры;
– частые «зависания» и сбои в работе компьютера.

Ложные антивирусы (также известные как «scareware») – это программы, которые внешне похожи на приложения для обеспечения безопасности компьютера, но в действительности такой защиты почти или совсем не обеспечивают, генерируют ошибочные или заведомо ложные уведомления об угрозах или пытаются вовлечь пользователя в мошеннические операции.

Антивирусные программы – специальные программы для обнаружения, уничтожения компьютерных вирусов и защиты от них. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как профилактические возможности, так и средства лечения от вирусов и восстановления данных.

Количество и разнообразие вирусов очень велико, поэтому, чтобы быстро и эффективно их обнаружить, антивирусная программа должна отвечать определенным требованиям:

– стабильность и надежность работы является определяющими параметрами, так как даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на компьютере, например, в результате какого-либо сбоя в работе программ процесс проверки компьютера не пройдет до конца. Тогда есть вероятность того, что какие-то зараженные файлы остались незамеченными;

– объем вирусной базы (количество обнаруживаемых программой вирусов) – с учетом постоянного появления новых вирусов база должна регулярно обновляться;

– скорость работы программы является одним из основных требований к любой антивирусной программе, так как огромный поток информации требует быстрой проверки файлов и дисков компьютера;

– наличие дополнительных возможностей, например алгоритмов определения неизвестных программе вирусов (эвристическое сканирование). Сюда же следует отнести умение работать с файлами различных типов (архивы, документы) и возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы. Немаловажным является наличие резидентного фильтра,

осуществляющего проверку всех файлов «на лету», т. е. автоматически, по мере их записи на диск;

– многоплатформенность (наличие версий программы под различные операционные системы).

Антивирусные программы выпускает ряд компаний. К наиболее распространенным относят следующие программы:

– программы-детекторы;
– программы-доктора, или фаги;
– программы-ревизоры;
– программы-фильтры;
– программы-вакцины, или иммунизаторы.

Наиболее распространены программы-доктора и программы-фильтры. А современные антивирусные пакеты включают все необходимые компоненты для противостояния любым вирусам. Например, «Антивирус Касперского» (Kaspersky Anti-Virus) содержит программу-фильтр Kaspersky Anti-Virus Monitor, программу-доктор Kaspersky Anti-Virus Scanner и программу-ревизор Kaspersky Anti-Virus Inspector.

Несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, необходимо создавать более универсальные и качественно новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. Защищенность от вирусов зависит и от грамотности пользователей.

Контрольные вопросы

1. Что такое компьютерный вирус?
2. Дайте определение ложным антивирусам.
3. Какие виды антивирусных программ существуют?
4. Расскажите классификацию компьютерных вирусов.
5. Какие бывают вирусы по среде обитания?

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).

2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).

3. Условие задания.

4. Исполнительская часть.

5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Установите и настройте антивирусную программу по варианту.

2. Обновите базу данных сигнатур вирусов.

3. Выполните сканирование дисков.

В электронный конспект поместите копии экрана с пояснениями всех проведенных действий.

Номер варианта	Антивирус
1	Avast! Free Antivirus
2	Kaspersky
3	AVG AntiVirus
4	Panda Cloud Antivirus
5	360 Total Security
6	Avira Free Antivirus
7	Zillya! Antivirus Free
8	Bitdefender Antivirus Free
9	Comodo Antivirus
10	Microsoft Security Essentials

Практическое занятие № 12

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ ДЛЯ РЕАЛИЗАЦИИ ПРИЛОЖЕНИЙ, ИСПОЛЬЗУЮЩИХ СИММЕТРИЧНОЕ И АССИМЕТРИЧНОЕ ШИФРОВАНИЕ, С ПРИМЕНЕНИЕМ БИБЛИОТЕКИ SYSTEM.SECURITY.CRYPTOGRAPHY

Цель: изучить модель криптографии .NET Framework, основные классы и структуры данных, разработать приложение для шифрования файлов, использующих симметричные и ассиметричные алгоритмы шифрования.

Теоретические сведения

В .NET Framework присутствует пространство имен для выполнения криптографических операций под названием System.Security.Cryptography. Данное пространство имен предоставляет криптографические службы, включающие безопасное кодирование и декодирование данных, а также другие операции, такие как хеширование сообщений, генерация случайных чисел и проверка подлинности сообщений. Данная библиотека предоставляет доступ для использования различных реализаций алгоритмов, в основном это программные интерфейсы CryptoApi (CAPI) и Cryptography Next Generation API (CNG API). Помимо этого, для некоторых алгоритмов возможно использование реализаций на основе OpenSSL.

CryptoAPI – интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером. Входит в состав операционных систем Microsoft. Большинство функций CryptoAPI поддерживается, начиная с Windows 2000.

Cryptography Next Generation API стала долгосрочной заменой CAPI. Данный набор интерфейсов поддерживает все алгоритмы, предлагаемые CAPI, а также другие алгоритмы, перечисленные в своде правил Suite B Агентства национальной безопасности США. Данный интерфейс поддерживает следующие длины ключей или размерность хеша:

– RSA от 512 до 16 384 бит с шагом 64 бит;

– DH – от 512 до 16 384 бит с шагом 64 бит;
– DSA – от 512 до 1024 бит с шагом 64 бит;
– ECDSA – P-256, P-384, P-521 (NIST Curves);
– ECDH – P-256, P-384, P-521 (NIST Curves);
– MD2 – 128 бит;
– MD4 – 128 бит;
– MD5 – 128 бит;
– SHA1 – 1160 бит;
– SHA256 – 256 бит;
– SHA384 – 384 бит;
– SHA512 – 512 бит.

Рассматривая структуру наследования для симметричных алгоритмов в .NET, стоит упомянуть, что SymmetricAlgorithm является абстрактным классом, от которого наследуются абстрактные классы для реализаций каждого из алгоритмов. В свою очередь каждая из реализаций алгоритма является производной от абстрактного класса алгоритма. Ниже представлена структура наследования:

SymmetricAlgorithm
    Aes
        AesCng
        AesManeged
        AesCryptoServiceProvider
    Des
        DesCng
        DesManeged
        DesCryptoServiceProvider
    TripleDes
        TripleDesCng
        TripleDesManeged
        TripleDesCryptoServiceProvider

Данная структура наследования повторяется для каждого из трех типов поддерживаемых криптографических операций: SymmetricAlgorithm, AsymmetricAlgorithm, HashAlgorithm.

Рассмотрим часть кода для шифрования сообщения с использованием алгоритма AES. Ниже показано создание объекта шифратора на основе созданного экземпляра криптографического объекта aesAlg и потоков для шифрования. Стоит отметить CryptoStream, который определяет поток, связывающий потоки данных с криптографическим преобразованием (листинг 1).

```
ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key,
aesAlg.IV);
 // создание потоков используемого для шифрования
using (MemoryStream msEncrypt = new MemoryStream())
{using (CryptoStream csEncrypt = new CryptoStream(msEncrypt,
encryptor, CryptoStreamMode.Write))
//1-используемый поток, 2 - криптографические преобразова-
ние, 3 тип доступа
{using (StreamWriter swEncrypt = new StreamWriter(csEncrypt))
{swEncrypt.Write(plainText);}
encrypted = msEncrypt.ToArray();} } }
```

Листинг 1. Шифрование сообщения с помощью алгоритма AES

Дешифрование выполняется аналогично, за исключением изменения типа доступа CryptoStream и изменения потока с записи на чтение (листинг 2).

```
ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key,
aesAlg.IV);
using (MemoryStream msDecrypt = new MemoryStream(cipherText))
{using (CryptoStream csDecrypt = new CryptoStream(msDecrypt,
decryptor, CryptoStreamMode.Read))
{using (StreamReader srDecrypt = new StreamReader(csDecrypt))
{plaintext = srDecrypt.ReadToEnd();} } }
```

Листинг 2. Дешифрование сообщения с помощью алгоритма AES

Также стоит упомянуть, что сложность большинства алгоритмов шифрования имеет сильную зависимость от длины ключа. Изменить длину ключа возможно в большинстве алгоритмов симметричного шифрования. Для изменения размера ключа необходимо изменить свойство KeySize (листинг 3).

```
using (TripleDES myDes = TripleDES.Create())
{myDes.KeySize = 128;
EncryptStringToFile_DES(route,    "2    keys    usedE.txt",
myDes.Key, myDes.IV);
DecryptStringToFile_DES("2    keys    usedE.txt",    "2    key
deceypted.txt", myDes.Key, myDes.IV);}
```

Листинг 3. Изменение размера ключа

Что касается ассиметричных алгоритмов, то они представлены в данной структуре наследования:

AsymmetricAlgorithm
    Rsa
        RsaCng
        RsaOpenSsl
        RsaCryptoServiceProvider
    Dsa
        DsaCng
        DsaOpenSsl
        DsaCryptoServiceProvider
    ECDiffieHellman
        ECDiffieHellmanCng
        ECDiffieHellmanOpenSsl

Шифрование и дешифрование для асимметричных алгоритмов выполнятся проще из-за встроенных функций Encrypt и Decrypt. Также стоит помнить, что RSA является блочным алгоритмом, и если длина данных не совпадает с длиной блока, то данные нужно дополнить до длины блока. Для этого в данном пространстве имен можно использовать разные режимы заполнения (листинг 4).

```
using (RSA myRsa = RSA.Create())
{string publickey = myRsa.ToXmlString(false);
//получим открытый ключ
string privatekey = myRsa.ToXmlString(true);
//получим закрытый ключ
byte[] encrypted = myRsa.Encrypt(data, RSAEncryptionPadding.Pkcs1);
byte[] decrypted = myRsa.Decrypt(encrypted,
RSAEncryptionPadding.Pkcs1);
Console.WriteLine("До шифрования: {0}", original);
Console.WriteLine("Зашифрованное: {0}",
System.Text.Encoding.UTF8.GetString(encrypted));
Console.WriteLine("После дешифровки: {0}",
System.Text.Encoding.UTF8.GetString(decrypted)); }
```

Листинг 4. Дополнение до длины блока

Как представлено в коде выше, после создания экземпляра RSA возможно сразу же зашифровать и дешифровать данные, используя автоматически сгенерированные ключи. Также код, представленный ниже, содержит пример для получения открытого и закрытого ключа в виде строки в формате Xml (листинг 5).

```
<RSAKeyValue>
<Modulus>6yEjtrItcUq1hoA01xc63EW5/P99kstIobXsxPCUfUODRn2daz
zcyhJ5Quhw1oHodlOMvtDN3xJdOTWDbH3xdQ==
</Modulus><Exponent>AQAB
</Exponent>
</RSAKeyValue>
```

Листинг 5. Получение открытого и закрытого ключа

Пример сохраненного в файл открытого ключа дан в листинге 6.

```
<RSAKeyValue>
<Modulus>6yEjtrItcUq1hoA01xc63EW5/P99kstIobXsxPCUfUODRn2daz
zcyhJ5Quhw1oHodlOMvtDN3xJdOTWDbH3xdQ==
</Modulus>
<Exponent>AQAB
</Exponent>
<P>9TsbWvgvA2OqPZxUZ96PomUG8rJk2T0SiH6chz65zkc=
</P>
<Q>9XR41YP8/CUoajovRPKWQZou3J23n3usp1acC3v9dGM=
</Q>
<DP>lnjHJ0GD72t3KUjETdu1fKrK4Z5u3RFpTtGJkD7/2b8=
</DP>
<DQ>9Qv2ppNCuigOlR7JmjflslDPgAklDN9XmyhoWT7L5qk=
</DQ>
<InverseQ>gSJ6G275fGFrEMqwSdgJYvmUQhnpCTcX0T3imIVQwOE=
</InverseQ>
<D>z0gMwu+6zehNtP/rFT9eXXd+qgHWAwYAxsapr0hjrzSXv1qS9QJJ+062
YbdHc24WZagrKqABfOLQ3hfLXP3JdQ==
</D></RSAKeyValue>
```

Листинг 6. Пример сохраненного файла

Как видно на представленных выше файлах, размеры открытого и закрытого ключей отличаются, но также совпадают modulus (n) и Exponent (e). Остальные параметры в закрытом ключе совпадают с общепринятыми обозначениями, кроме DP=d mod (p-1), DQ=d mode (q-1) и D, обозначающего r или закрытый показатель степени.

Хеширование в .NET выполняется проще остальных операций из-за отсутствия необходимости в обратном преобразовании. В данном пространстве имен поддерживаются следующие алгоритмы:

– MD5;
– SHA256;
– SHA384;
– SHA512.

Пример кода представлен в листинге 7.

```
    byte[] hashValue = new byte[256];
    using (SHA256 mysha256 = SHA256.Create())
    {hashValue=mysha256.ComputeHash(File.ReadAllBytes("sha.
txt"));
    File.WriteAllBytes("hash.txt", hashValue);}
```

Листинг 7. Хеширование

Как видно из представленного кода, после инициализации экземпляра для шифрования нужно вызвать только один метод ComputeHash, который выполнит хеширование данных.

Пример захешированных данных представлен на рис. 27.

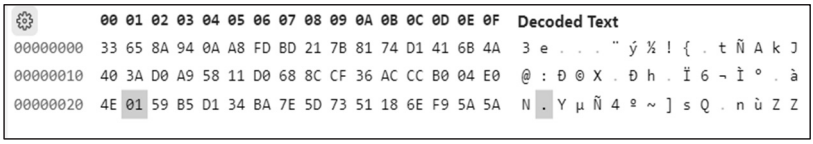

Рис. 27. Пример захешированных данных

Контрольные вопросы

1. Назовите основное назначение библиотеки System.Security.Cryptography.
2. Что из себя представляет интерфейс CryptoApi?
3. Что такое Cryptography Next Generation?

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).
2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).
3. Условие задания.
4. Исполнительская часть.
5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Ознакомьтесь с созданием криптографического приложения.

2. Выполните шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам. Используя функции работы с файлами, сохраните ключи шифрования, результаты шифрования и хеширования.

3. Для выше указанных алгоритмов, используя Hex-редактор, продемонстрируйте ключи шифрования, зашифрованные и захешированные данные.

4. Реализуйте проверку сообщения (фамилии) и хеша по примеру ЭЦП. Продемонстрируйте, что произойдет, если будет изменен хеш или сообщение. Задания того, что нужно реализовать, представлены ниже.

Номер варианта	Алгоритм шифрования (размер ключа)	Алгоритм хеширования
1	AES (128 бит)	SHA256
2	DES	SHA1
3	TripleDes (128 бит)	SHA384
4	RSA (512 бит)	MD5
5	AES (192 бит)	SHA1
6	DES	SHA256
7	TripleDes (192 бит)	SHA384
8	RSA (1024 бит)	SHA256
9	AES (256 бит)	SHA512
10	DES	SHA384
11	TripleDes (128 бит)	SHA1
12	RSA (640 бит)	SHA384
13	AES (128 бит)	SHA384
14	DES	SHA512
15	TripleDes (128 бит)	SHA1
16	RSA (2048 бит)	SHA512
17	AES (192 бит)	SHA1
18	DES	MD5
19	TripleDes (192 бит)	SHA256
20	RSA (4096 бит)	MD5
21	AES (256 бит)	MD5
22	DES	SHA1
23	TripleDes (128 бит)	SHA256
24	RSA (576 бит)	SHA1
25	AES (128 бит)	SHA1
26	DES	SHA256
27	TripleDes (128 бит)	MD5
28	RSA (1088 бит)	SHA512
29	AES (192 бит)	SHA384
30	RSA (1536 бит)	SHA256

Практическое занятие № 13

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ ДЛЯ РЕАЛИЗАЦИИ СИММЕТРИЧНОГО И АССИМЕТРИЧНОГО ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ SUBTLECRYPTO В JS

Цель: изучить интерфейс SubtleCrypto, основные классы и структуры данных: разработать приложение для шифрования файлов, использующих симметричные и ассиметричные алгоритмы шифрования.

Теоретические сведения

Криптография в JS. Web Crypto API – это интерфейс, позволяющий использовать криптографические примитивы для построения систем с использованием криптографии. Данный интерфейс включает в себя возможность генерировать, использовать и применять пары криптографических ключей, шифровать и дешифровать сообщения, надежно генерировать случайные числа.

Некоторые браузеры реализовали интерфейс под названием Crypto без точной структуры. Чтобы избежать путаницы, методы и свойства этого интерфейса были удалены из браузеров, реализующих Web Crypto API, и все методы Web Crypto API доступны в новом интерфейсе: SubtleCrypto.

Интерфейс SubtleCrypto Web Crypto API предоставляет ряд низкоуровневых криптографических функций. Доступ к функциям SubtleCrypto осуществляется через объект Crypto.subtle.

Этот объект содержит набор методов для выполнения общих криптографических функций, таких как шифрование, хеширование, подписывание и генерация ключей. Поскольку все криптографические операции выполняются с необработанными двоичными данными, каждый метод SubtleCrypto имеет дело с типами ArrayBuffer и ArrayBufferView. Из-за того что строки нередко становятся предметом криптографических операций, классы TextEncoder и TextDecoder будут часто использоваться вместе с SubtleCrypto для преобразования в строки и обратно.

Одной из проблем криптографии является генерация случайных чисел. Если будет использовать Math.random(), сгенерируется псевдослучайное число, которое использует генератор PRNG (pseudorandom number generator). Поскольку сгенерированное число находится внутри PRNG, то использование данного алгоритма для криптографии неприемлемо. Решить эту проблему позволит криптографически безопасный генератор псевдослучайных чисел (cryptographically secure pseudorandom number generator, CSPRNG), который дополнительно включает в себя источник энтропии в качестве входных данных таких системных свойств, которые проявляют непредсказуемое поведение. Этот алгоритм медленнее PRNG, но значения, генерируемые CSPRNG, являются достаточно непредсказуемыми для криптографических целей. Код для генерации нескольких случайных чисел показан в листинге 8.

```
const array = new Uint8Array(1);
for (let i=0; i<5; ++i) {
 console.log(crypto.getRandomValues(array));}
```

Листинг 8. Код генерации случайных чисел

Хеширование. Хеширование в SubtleCrypto представлено следующими алгоритмами:

– SHA1;
– SHA256;
– SHA385;
– SHA512.

Метод SubtleCrypto.digest() используется для создания хеша сообщения. Пример для хеширования сообщения представлен в листинге 9.

```
const text = 'Hash using sha256';
async function digestMessage(message) {
 const encoder = new TextEncoder();
 const data = encoder.encode(message);
 const hash = await crypto.subtle.digest('SHA-256', data);
 return hash;}
digestMessage(text)
 .then((digestBuffer)                                          =>
console.log(digestBuffer.byteLength));
```

Листинг 9. Пример хеширования данных

Как видно из примера выше, для указания алгоритма хеширования применяется первый параметр. Также стоит упомянуть, что результат хеширования обычно используется в 16-ричной форме. Для преобразования стоит добавить код, представленный в листинге 10.

```
const hashArray = Array.from(new Uint8Array(hash));
const hashHex = hashArray.map((b) =>
b.toString(16).padStart(2, '0')).join('');
return hashHex;
```

Листинг 10. Пример преобразование хеша в 16-ричную форму

Генерация ключей. Генерация случайного ключа CryptoKey выполняется с помощью метода SubtleCrypto.generateKey (algorithm, extractable, keyUsages). В этот метод передается объект params, отображающий целевой алгоритм, логическое значение, указывающее, должен ли ключ извлекаться из объекта CryptoKey, и массив строк keyUsages, отмечающий , с какими методами будет взаимодействовать.

Поскольку разные алгоритмы используют разный набор данных для ключей, то первый параметр содержит соответствующее название алгоритма:

– RSA (RSASSA-PKCS1-v1_5, RSA-PSS, or RSA-OAEP) использует объект RsaHashedKeyGenParams.

– ECDSA и ECDH используют объект EcKeyGenParams.

– HMAC использует объект HmacKeyGenParams.

– AES (AES-CTR, AES-CBC, AES-GCM, AES-KW) использует объект AesKeyGenParams

Значение extractable является логическим значением и указывает на возможность экспорта ключа.

Третий параметр keyUsages описывает, с какими алгоритмами можно использовать ключ:

– encrypt: ключ используется для шифрования сообщений;

– decrypt: ключ используется для расшифровки сообщений;

– sign: ключ используется для подписи сообщений;

– verify: ключ используется для проверки подписанного сообщения;

– deriveKey: ключ используется для получения ключа;

– deriveBits: ключ используется для получения битов;

– wrapKey: ключ используется для упаковки ключа;

– unwrapKey: ключ используется для распаковки ключа.

Пример генерация ключа представлен в листинге 11.

```
(async function() {
 const params = {
 name: 'AES-CTR',
 length: 128 };
 const keyUsages = ['encrypt', 'decrypt'];
 const key = await crypto.subtle.generateKey(params, false,
keyUsages);
 console.log(key);};
```

Листинг 11. Пример генерации ключа

Шифрование и дешифрование. Объект SubtleCrypto позволяет использовать как открытый ключ, так и симметричные алгоритмы для шифрования и дешифрования сообщений. Оно может быть выполнено с использованием методов SubtleCrypto.encrypt() и SubtleCrypto.decrypt() соответственно. Ниже представлена часть кода для шифрования и дешифрования данных, где algoIdentifier – это название алгоритма (листинг 12).

```
const originalPlaintext = (new TextEncoder()).encode('Crypto');
 const encryptDecryptParams = {
 name: algoIdentifier,
 iv: crypto.getRandomValues(new Uint8Array(16)) };

 const ciphertext = await crypto.subtle.encrypt(encryptDecryptParams, key,
 originalPlaintext);

 console.log(ciphertext);
 const decryptedPlaintext = await crypto.subtle.decrypt(encryptDecryptParams,
 key, ciphertext);

 console.log((new TextDecoder()).decode(decryptedPlaintext));
```

Листинг 12. Часть кода для шифрования и дешифрования

Создание цифровой подписи и проверка сообщений. Объект SubtleCrypto позволяет применять алгоритмы с открытым ключом для генерации подписей с использованием закрытого ключа или для проверки подписей с использованием открытого ключа. Они

выполняются методами SubtleCrypto.sign() и SubtleCrypto.verify() соответственно. Для подписания сообщения требуется объект params, чтобы указать алгоритм и любые необходимые значения, частный CryptoKey и ArrayBuffer или ArrayBufferView для подписи. В примере, представленном в листинге 13, можно увидеть процесс создания цифровой подписи и проверки сообщения с цифровой подписью (листинг 13).

```
 async function() {
 const keyParams = {
 name: 'ECDSA',
 namedCurve: 'P-256'
};
 const keyUsages = ['sign', 'verify'];
 const       {publicKey,       privateKey}       =       await
crypto.subtle.generateKey(keyParams,
 true, keyUsages);

 const message = (new TextEncoder()).encode('Mes to sign');
 const signParams = {
 name: 'ECDSA',
 hash: 'SHA-256' };
 const   signature   =   await   crypto.subtle.sign(signParams,
privateKey, message);
 const   verified   =   await   crypto.subtle.verify(signParams,
publicKey, signature, message);
 console.log(verified);
})();
```

Листинг 13. Пример создания и проверки сообщений с цифровой подписью

Упаковка и распаковка ключа. Объект SubtleCrypto позволяет упаковывать и распаковывать ключи, чтобы обеспечить передачу по ненадежному каналу. Это выполняется с использованием методов SubtleCrypto.wrapKey() и SubtleCrypto.unwrapKey() соответственно. Для переноса ключа требуется строка форматирования, экземпляр CryptoKey для переноса, CryptoKey для выполнения переноса и объект params для указания алгоритма и любых необходимых значений. В примере, представленном в листинге 14, симметричный ключ AES-GCM упаковывается с помощью AES-KW и распаковывается обратно.

```
 (async function() {
 const keyFormat = 'raw';
 const extractable = true;
 const wrappingKeyAlgoIdentifier = 'AES-KW';
 const wrappingKeyUsages = ['wrapKey', 'unwrapKey'];
 const wrappingKeyParams = {
 name: wrappingKeyAlgoIdentifier,
 length: 256};
 const keyAlgoIdentifier = 'AES-GCM';
 const keyUsages = ['encrypt'];
 const keyParams = {
 name: keyAlgoIdentifier,
 length: 256};
 const wrappingKey = await crypto.subtle.generateKey(wrappingKeyParams,
 extractable, wrappingKeyUsages);
 console.log(wrappingKey);
const key = await crypto.subtle.generateKey(keyParams,
extractable, keyUsages);
 console.log(key);
const wrappedKey = await crypto.subtle.wrapKey(keyFormat,
key, wrappingKey,
 wrappingKeyAlgoIdentifier);
 console.log(wrappedKey);
const unwrappedKey = await crypto.subtle.unwrapKey(keyFormat,
wrappedKey,
 wrappingKey, wrappingKeyParams, keyParams, extractable,
keyUsages);
 console.log(unwrappedKey);})()
```

Листинг 14. Пример упаковки и распаковки ключа

Контрольные вопросы

1. Что из себя представляет интерфейс Web Crypto API?
2. Опишите особенности работы объекта SubtleCrypto.

Оформление отчета по заданию

1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть).

2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы).

3. Условие задания.

4. Исполнительская часть.

5. Использованные источники (нормативные документы, сайты, учебники и т. п.).

Задание для выполнения

1. Ознакомьтесь с созданием криптографического приложения.

2. Выполните генерацию и вывод в консоль случайный чисел.

3. Выполните шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам.

Номер варианта	Алгоритм шифрования (размер ключа)	Алгоритм хеширования
1	RSA-OAEP	SHA1
2	AES-CTR	SHA256
3	AES-CBC	SHA384
4	AES-GCM	SHA512
5	AES-CTR	SHA1
6	AES-CBC	SHA256
7	AES-GCM	SHA384
8	RSA-OAEP	SHA512
9	AES-CBC	SHA1
10	AES-GCM	SHA256
11	RSA-OAEP	SHA384
12	AES-CTR	SHA512
13	AES-GCM	SHA1
14	RSA-OAEP	SHA256
15	AES-CTR	SHA384

Если количество человек в группе больше 15, то номер варианта определяется как $x = n \bmod 15$, где n – номер в списке. Если номер варианта в ходе решения уравнения равен 0, то номер варианта равен 15.

4. Продемонстрируйте упаковку и распаковку ключа, полученного в предыдущем задании, используя алгоритм AES-KW.

5. Выполните процедуру подписи сообщения и проверку подлинности с использованием RSA-PSS или ECDSA на выбор.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Урбанович, П. П. Информационная безопасность и надежность систем: учеб.-метод. пособие для студентов специальности 1-40 01 02-03 «Информационные системы и технологии» / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск: БГТУ, 2007. – 90 с.

2. Урбанович, П. П. Защита информации и надежность информационных систем: пособие для студентов специальности 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)» / П. П. Урбанович, Д. В. Шиман. – Минск: БГТУ, 2014. – 91 с.

3. Урбанович, П. П. Избыточность в полупроводниковых интегральных микросхемах памяти / П. П. Урбанович, В. Ф. Алексеев, Е. А. Верниковский. – Минск: Навука і тэхніка, 1995. – 262 с.

4. Смелов, В. В. Методологические основы информационной безопасности автоматизированных систем / В. В. Смелов // Труды БГТУ. Серия VI, Физико-математические науки и информатика. – 2009. – Вып. XVII. – С. 126–131.

5. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; под ред. В. Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.

6. Кудашов, В. И. Интеллектуальная собственность: охрана и реализация прав, управление: учеб. пособие / В. И. Кудашов. – Минск: БНТУ, 2004. – 321 с.

7. Якимахо, А. П. Управление объектами интеллектуальной собственности / А. П. Якимахо, Г. И. Олехнович. – Минск: ГИУСТ БГУ, 2006. – 472 с.

8. Безбогов, А. А. Методы и средства защиты компьютерной информации: учеб. пособие / А. А. Безбогов, А. В. Яковлев, В. Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.

9. Математические и компьютерные основы криптологии: учеб. пособие / Ю. С. Харин [и др.]. – Минск: Новое знание, 2003. – 382 с.

10. Основы криптографии: учеб. пособие / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2001. – 480 с.

11. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М.: ДМК Пресс, 2000. – 448 с.

12. Тимошенко, А. А. Защита информации в специализированных информационно-телекоммуникационных системах: текст лекций / А. А. Тимошенко. – Киев: КПИ, 2010. – 251 с.

13. Шилдт, Г. C# 4.0. Полное руководство: пер. с англ. / Г. Шилдт. – М.: И. Д. Вильямс, 2019. – 1056 с.

14. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, 1997. – 368 с.

15. Макаренко, С. И. Информационная безопасность: учеб. пособие / С. И. Макаренко. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

16. Нестеров, С. А. Информационная безопасность и защита информации: учеб. пособие / С. А. Нестеров. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

ОГЛАВЛЕНИЕ

Учебное издание

Ржеутская Надежда Викентьевна
Нистюк Ольга Александровна
Уласевич Николай Иванович

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторный практикум

Учебно-методическое пособие

Редактор *О. П. Приходько*
Компьютерная верстка *Е. В. Ильченко*
Дизайн обложки *Д. А. Полешова*
Корректор *О. П. Приходько*

Подписано в печать 11.01.2024. Формат 60×84 1/16.
Бумага офсетная. Гарнитура Таймс. Печать ризографическая.
Усл. печ. л. 7,2. Уч.-изд. л. 7,4.
Тираж 120 экз. Заказ .

Издатель и полиграфическое исполнение:
УО «Белорусский государственный технологический университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/227 от 20.03.2014.
Ул. Свердлова, 13а, 220006, г. Минск.