Вопрос 6. Испытания средств защиты информации

1. Типы сертификационных испытаний

Сертификационные испытания:

- технических средств защиты информации;
- защищенных технических средств обработки информации;
- технических средств контроля эффективности защиты информации;
- программных средств защиты информации от несанкционированного доступа (НСД);
- защищенных от НСД программных средств обработки информации;
- программных средств контроля защищенности информации от НСД.

Виды проводимых сертификационных испытаний:

- на соответствие требованиям нормативных и руководящих документов ФСТЭК России по защите информации от несанкционированного доступа;
- на соответствие требованиям нормативных и руководящих документов ФСТЭК России по защите информации от ее утечки по техническим каналам;
- на соответствие требованиям стандарта ГОСТ Р ИСО/МЭК 15408-2002.

Схемы проводимых сертификационных испытаний:

- сертификация единичного образца продукции;
- сертификация партии идентичных образцов продукции с фиксированным тиражом копий;
- сертификация процесса производства идентичных образцов продукции с открытым тиражом копий в течении срока действия сертификата, включающая сертификационные испытания единичного образца продукции и экспертизу процесса производства сертифицируемой продукции. <1>

<1> Услуга Сертификационные испытания средств защиты информации (URL: http://www.geyser-telecom.ru/rus/services/full/sertificatsiya/sertif_inf_secuirity/). 2018.

2. Порядок проведения сертификационных испытаний

При изучении технологического процесса автоматизированной обработки и хранения информации обращается внимание на такие компоненты объекта ВТ как объекты и субъекты доступа, средства обработки и передачи информации:

- к объектам доступа относятся средства обработки и передачи информации, информационные носители на магнитной и бумажной основе, накопители и все виды памяти ЭВМ, в которых может находиться информация, отдельные документы и их архивы, используемые в технологическом процессе автоматизированной обработки информации, файлы, записи и другие единицы информационных ресурсов, доступ к которым необходимо регламентировать;
- к субъектам доступа относятся персонал и все лица, которые имеют возможность доступа к средствам обработки информации, а также программные средства, посредством которых осуществляется доступ к объектам;
- к средствам обработки и передачи информации относятся технические и программные средства ВТ, средства и линии связи, предоставляющие возможности как для перемещения (копирования) информации между различными областями памяти и

информационными носителями, различными средствами обработки, определенными для объекта ВТ, так и по выводу информации из установленной для нее сферы обращения.

Используя исходные данные по технологии обработки и передачи информации, разрешительной системы доступа персонала к защищаемым ресурсам, анализируется обобщенная технологическая схема объекта ВТ с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

Проверяется соответствие описания технологического процесса обработки, хранения и передачи конфиденциальной информации реальной практике на объекте.

Проверяются паспортные (исходные) данные объекта ВТ и устанавливаются опасные факторы и угрозы, критические места объекта ВТ, снижающие уровень защиты, комплектность и характеристики средств защиты.

Проверяются наличие оформленных разрешений на допуск персонала к информации определенного уровня конфиденциальности, метки конфиденциальности (грифа секретности) на информационных носителях, соответствие технологических инструкций пользователей и администратора безопасности информации установленным требованиям.

По результатам изучения уточняется схема технологического процесса с привязкой к конкретным средствам обработки и передачи информации и штатному персоналу.

1) Проверка на соответствие организационно-техническим требованиям по защите информации.

Проверка объекта ВТ на соответствие организационно-техническим требованиям по защите информации проводится в объеме, указанном в таблице.

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации	9.4.2
Проверка соответствия состава и структуры программно-технических средств объекта ВТ представленной документации	9.4.3
Проверка правильности классификации объекта ВТ	9.4.4
Проверка правильности категорирования объектов ВТ	9.4.5
Проверка уровня подготовки кадров и распределения ответственности персонала	9.4.6
Проверка наличия сертификатов соответствия на СВТ и средства защиты информации, экспертиза отчетов и протоколов по специальным исследованиям СВТ, предписаний на эксплуатацию СВТ	9.4.7
Проверка выполнения требований к помещениям, в которых производится обработка информации средствами ВТ	9.4.8

Проверка на соответствие организационно-техническим требованиям по защите информации

Производится проверка достаточности представленных документов и соответствия их содержания требованиям стандартов и иных руководящих документов по безопасности информации Гостехкомиссии России и других органов государственного управления в пределах компетенции.

Состав и структура программно-технических средств, включенных в реальный технологический процесс обработки информации, сверяется с представленной документацией.

Проверка правильности классификации ВТ производится в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» и раздела 6 СТР на основании следующих определяющих признаков:

- уровней конфиденциальности (степени секретности) обрабатываемой информации;
- уровней полномочий по доступу к конфиденциальной информации различных пользователей;
- режимов обработки данных на объекте ВТ - многопользовательский или однопользовательский;
- максимального уровня конфиденциальности обрабатываемой информации. Полученный класс объекта ВТ сравнивается с установленным на объекте аттестации.

Проверка правильности категорирования объектов ВТ производится в соответствии с требованиями раздела 3 СТР на основании следующих исходных данных:

- максимального уровня конфиденциальности (степени секретности) обрабатываемой на объекте ВТ информации;
- условий расположения объекта ВТ.

Указанные исходные данные должны быть подтверждены документально заключениями об уровне конфиденциальности информации, актами, планами размещения и другими документами.

Производится категорирование объектов ВТ. Результаты категорирования сравниваются с категориями, указанными в актах категорирования соответствующих объектов ВТ.

Проверка уровня подготовки кадров и распределения ответственности производится на основе следующих показателей:

- экспертной оценки знания инструкций по безопасности информации пользователями и эксплуатационным персоналом;
- наличия разрешительной системы доступа персонала к защищаемым ресурсам, определяющей полномочия по доступу к конфиденциальной информации и процедуры их оформления, системы распределения ответственности персонала за выполнение требований по безопасности информации, оформленной приказами и распоряжениями руководителя предприятия (объекта информатизации);
- экспертной оценки системы технической учебы и повышения квалификации персонала и пользователей объекта ВТ.

Путем опроса персонала проверяется доведение до конкретных исполнителей руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях.

Производится проверка наличия документов, подтверждающих возможность применения технических и программных средств ВТ, средств защиты для обработки конфиденциальной информации (сертификатов соответствия), экспертиза отчетов и протоколов по специальным исследованиям СВТ, предписаний на эксплуатацию СВТ, а также их соответствия требованиям нормативных документов.

При проверке помещений производится оценка их соответствия требованиям действующей инструкции по обеспечению режима секретности в министерствах, ведомствах, на предприятиях.

Производится проверка выполнения требований руководящих документов по условиям размещения СВТ в рабочих помещениях, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

Если средства ВТ установлены в выделенных помещениях, то проверяются документы, подтверждающие защищенность информации в этих средствах от утечки за счет электроакустических преобразований в соответствии с требованиями раздела 4 СТР.

По результатам проверки комиссия должна сделать выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям по безопасности информации.

2) Испытания на соответствие требованиям по защите информации от утечки по каналам ПЭМИН.

Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.

Проверка проводится в объеме, указанном в таблице.

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка соответствия фактических размеров контролируемой зоны представленным документам	9.5.1.2
Проверка соответствия размеров контролируемой зоны требованиям предписаний на эксплуатацию СВТ и других документов, определяющих требования к размеру зоны 2	9.5.1.3
Проверка работоспособности средств защиты информации, выполнения правил их эксплуатации	9.5.1.4
Экспертная оценка результатов аппаратурного контроля защищенности СВТ	9.5.1.5
Аппаратурные испытания эффективности защиты информации от утечки за счет ПЭМИН СВТ	9.5.1.6

Испытания на соответствие требованиям по защите информации от утечки по каналам ПЭМИН

Производится выборочная проверка соответствия размеров контролируемой зоны (КЗ) в представленных документах (планы объекта, планы размещения СВТ, акты обследования и др.) **фактическим размерам контролируемой зоны**. Определяются минимальные значения расстояний от источников информативных сигналов до границы КЗ.

Сравниваются требуемые значения расстояний до границы КЗ, указанные в предписаниях на эксплуатацию СВТ (радиусы зоны 2), с фактическими значениями этих расстояний. Значения R2 должны укладываться в расстояния от СВТ до границ КЗ. В противном случае должны применяться дополнительные меры и средства защиты.

Проверка средств защиты информации производится по следующим показателям:

- соответствие видов и типов установленных средств защиты тем, что указаны в предписаниях на эксплуатацию СВТ (САЗ, экранирующие конструкции, фильтры);
- наличие сертификатов соответствия на средства защиты;
- выполнение правил монтажа и эксплуатации средств защиты;
- наличие актов ввода в эксплуатацию и протоколов контроля средств защиты;
- работоспособность средств защиты.

Производится экспертная оценка результатов контроля эффективности защиты информации в СВТ по следующим признакам:

- использованные методики контроля;
- использованные тестовые средства;
- полнота проведенных измерений по объему и видам измерений (частотный спектр, режимы работы СВТ, измеренные составляющие электромагнитного поля, направления распространения информативных сигналов в пространстве);
- использованная измерительная аппаратура;
- схема измерений;

- достоверность результатов измерений.

Аппаратурные испытания защищенности информации от утечки за счет ПЭМИ СВТ производятся выборочно для отдельных СВТ в соответствии с действующими нормами эффективности защиты информации от утечки за счет ПЭМИН, методикой контроля защищенности объектов ВТ, методиками специальных исследований СВТ, утвержденными (согласованными) Гостехкомиссией России.

3) Проверка выполнения требований по защите информации от утечки за счет наводок на вспомогательные средства и системы.

Проверка проводится в объеме, указанном в таблице.

Производится проверка **выполнения требований по размещению вспомогательных технических средств** и систем (ВТСС), имеющих выход за пределы контролируемой зоны объекта, на расстояниях не менее чем r и r' от основных технических средств и систем (ОТСС), обрабатывающих конфиденциальную информацию, где r и r'- требуемые в соответствии с разделом 5 СТР минимальные расстояния, согласно предписаниям на эксплуатацию СВТ.

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка взаимного размещения СВТ и вспомогательных средств на соответствие требованиям предписания на эксплуатацию СВТ и других документов, определяющих размеры зон r и r'	9.5.2.2
Проверка работоспособности средств защиты, выполнения правил их монтажа и эксплуатации	9.5.1.4
Экспертная оценка результатов аппаратурного контроля защищенности информации	9.5.1.6
Аппаратурные испытания защиты информации от утечки за счет наводок на вспомогательные средства и системы	9.4.2.3

Проверка выполнения требований по защите информации от утечки за счет наводок на вспомогательные средства и системы

Производятся выборочные аппаратурные испытания защищенности информации от утечки за счет наводок на ВТСС в соответствии с методиками, утвержденными (согласованными) Гостехкомиссией России.

4) Проверка выполнения требований по защите информации от утечки по цепям заземления и электропитания.

Проверка проводится в объеме, указанном в таблице.

Наименование проверок и испытаний	Пункт методических рекомендаций
Проверка выполнения требований к схеме организации электропитания технических средств ВТ, монтажу питающих кабелей, фильтрации опасных сигналов в цепях питания	9.5.3.2
Проверка выполнения требований руководящих документов по выполнению схемы заземления, правилам монтажа заземляющих конструкций, величине сопротивления заземлителя и регламентному контролю его значении	9.5.3.3
Проверка работоспособности использованных в составе объекта ВТ средств защиты информации, выполнения правил их монтажа и эксплуатации	9.5.1.4
Экспертная оценка результатов контроля эффективности мер и средств защиты информации в цепях электропитания и заземления	9.5.1.5
Аппаратурные испытания эффективности защиты информации от утечки по цепям заземления и электропитания средств ВТ	9.5.3.4

Проверка выполнения требований по защите информации от утечки по цепям заземления и электропитания

Производится проверка выполнения требований разделов 9 и 10 СТР по выполнению схемы энергопитания средств ВТ:

- по размещению трансформаторной подстанции;
- по монтажу фидерных линий, их экранированию и фильтрации;
- по монтажу САЗ и сетевых фильтров.

Производится проверка выполнения следующих требований:

- по размещению очага заземления и величине его сопротивления;
- наличию протоколов измерения величины сопротивления току растекания очага заземления;
- отсутствию соединений системы заземления с металлоконструкциями, выходящими за пределы контролируемой зоны.

Производятся выборочные аппаратурные испытания защищенности информации от утечки по цепям заземления и электропитания СВТ в соответствии с методиками, утвержденными (согласованными) Гостехкомиссией России.

Проверка выполнения требований по защите информации от утечки по кабельным линиям передачи данных СВТ и сетей связи.

Комплексные испытания объекта ВТ на соответствие требованиям по защите информации от утечки за счет ПЭМИН.

Комплексные испытания объекта ВТ проводятся в рабочих эксплутационных режимах технических средств и средств защиты информации. При этом оценивается работоспособность средств защиты информации, а также средств контроля и сигнализации и их электромагнитная совместимость со средствами обработки информации.

В процессе испытаний по выбору комиссии могут моделироваться нештатные ситуации, связанные с выходом из строя средств защиты и т.п.

5) Рекомендации по результатам испытаний.

По результатам испытаний должны быть сделаны выводы о соответствии (или несоответствии) объекта ВТ требуемому уровню защиты информации от утечки за счет ПЭМИН СВТ.

Комиссия может рекомендовать следующие меры по устранению недостатков:

- применение дополнительных организационных и технических мер по защите информации;
- применение дополнительных сертифицированных средств защиты информации;
- исключение отдельных технических средств, обрабатывающих конфиденциальную информацию, из состава объекта.

6) Проверка выполнения требований по защите информации от утечки за счет специальных электронных устройств перехвата информации.

Проверяется наличие актов или заключений о специальной проверке импортных СВТ, применяемых для обработки секретной информации.

7) Испытания на соответствие требованиям по защите информации от несанкционированного доступа.

Испытания проводятся в объеме, указанном в таблице.

Объем испытаний на соответствие требованиям по ЗИ от НСД может уточняться в зависимости от установленного класса АС.

Наименование проверок и испытаний	Пункт методических рекомендаций
Анализ и оценка технологического процесса обработки информации	9.7.2
Выбор инструментальных средств и методики испытаний	9.7.3
Испытания подсистемы управления доступом	9.7.4
Проверка механизма идентификации	9.7.4.1-9.7.4.2
Проверка механизма аутентификации	9.7.4.3-9.7.4.4
Проверка механизма контроля доступа	9.7.4.5
Проверка механизмов управления потоками информации	9.7.4.6-9.7.4.7
Испытания подсистемы регистрации и учета	9.7.5
Испытания подсистемы обеспечения целостности	9.7.6

Испытания на соответствие требованиям по защите информации от несанкционированного доступа

Анализ и оценка технологического процесса обработки информации в части НСД.

Комиссии представляется описание технологического процесса обработки информации в аттестуемом объекте ВТ, включающее в себя следующую информацию:

- перечень объектов доступа;
- перечень субъектов доступа;
- перечень штатных средств доступа к информации на объекте ВТ;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков.

В качестве объектов доступа в зависимости от класса СВТ могут быть приняты:

- система в целом;
- терминалы, ЭВМ, узлы сети ЭВМ, каналы связи, внешние устройства ЭВМ;
- программы;
- тома, каталоги, файлы, записи, поля записей;
- все виды памяти ЭВМ, в которых может находиться информация.

Информационные носители могут иметь метку конфиденциальности (гриф секретности) и находиться на учете.

В качестве субъектов доступа могут рассматриваться лица и процессы (программы пользователей), имеющие возможность доступа к объектам штатными средствами объекта ВТ.

Субъекты доступа могут иметь официальное разрешение (допуск) к информации определенного уровня конфиденциальности.

Под штатными средствами доступа к информации на объекте ВТ понимаются общесистемные и прикладные системы, средства и программы, предоставляющие субъектам документированные возможности доступа к объектам доступа.

Комиссия проверяет соответствие описания технологического процесса обработки и хранения конфиденциальной информации реальному процессу.

Особое внимание уделяется выявлению возможностей переноса информации большего уровня конфиденциальности на информационный носитель меньшего уровня.

Проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретным СВТ и штатному персоналу, оценка их

соответствия разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки.

8) Выбор методики испытаний и инструментальных средств.

Методика испытаний АС на соответствие требованиям защиты информации от НСД уточняется на основании результатов анализа технологического процесса обработки информации в АС

Методика испытаний должна включать в себя перечень инструментальных средств, используемых при испытаниях и проверках данной АС.

Методика испытаний может дополняться, уточняться и корректироваться в процессе испытаний руководителем аттестационной комиссии по согласованию с заявителем.

В качестве тестирующих средств для проведения испытаний могут быть выбраны технические и программные средства, принятые в установленном порядке для такого рода деятельности.

Перечень принятых тестирующих средств с описанием их возможностей и местонахождения хранится в органе по аттестации объектов информатики и предоставляется для ознакомления заинтересованным сторонам.

При отсутствии необходимых тестирующих средств они могут быть специально разработаны в период проведения аттестационных испытаний. Возможность их применения при испытаниях подтверждается председателем аттестационной комиссии и согласовывается с заявителем. После окончания испытаний документация на эти тестирующие средства прилагается к протоколам испытаний и отсылается в орган по аттестации.

9) Испытания подсистемы управления доступом.

Проверка правильности идентификации объектов доступа в АС проверяется путем обращения к ним субъектов доступа по идентификаторам объектов. Обращение должно осуществляться однозначно только к данному объекту.

Объекты доступа определяются в соответствии с РД Гостехкомиссии России «Автоматизированные системы Защита от НСД к информации. Классификация АС и требования по защите информации» и актом классификации АС.

Проверка правильности идентификации субъектов доступа проверяется путем обращения субъектов доступа АС к объектам доступа при помощи штатных средств.

При обращении должна проводиться проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных в АС идентификаторов субъектов.

Если субъект доступа предъявляет идентификатор, не известный системе, то средства управления должны прекращать процесс предоставления доступа.

При подтверждении подлинности (аутентификации) проверяется действительная принадлежность субъекту доступа предъявленного им идентификатора.

В качестве идентификатора могут быть использованы, например, биометрические признаки субъекта, специальные устройства (магнитная карточка, жетон и т.д.), пароль временного действия.

При проверке надежности аутентификации должна оцениваться вероятность подбора или несанкционированного получения (хищения) секретного (личного) признака или устройства посторонним субъектом доступа за период действия этого признака (устройства).

Правильность определения системой полномочий и предоставления доступа субъектам по отношению к объектам проверяется следующим образом.

По описанию применения СЗИ выявляются виды полномочий (читать, изменять, выполнять, передавать и т.д.), по которым различаются права субъектов на доступ к объектам. Проверяется правильность предоставления доступа в соответствии с установленными правами субъектов по отношению к конкретным объектам.

Управление потоками информации осуществляется на основании сопоставления меток конфиденциальности объектов доступа. Необходимо проверить наличие меток конфиденциальности на всех информационных объектах доступа. Метки конфиденциальности (грифы) должны быть ранжированы по важности помечаемой информации.

Наличие и надежность средств управления потоками информации в АС проверяется путем моделирования информационных потоков в реальном технологическом процессе по всем выявленным средствам перемещения информации. В АС должен блокироваться перенос информации с более высоким уровнем конфиденциальности на объекты с меньшим уровнем.

10) Испытания подсистемы регистрации и учета.

Регистрация и учет событий, определенных требованиями по безопасности информации к установленному классу АС, должны производиться на всех этапах технологического процесса хранения и обработки конфиденциальной информации. Регистрация должна охватывать все события, определенные указанным РД Гостехкомиссии России для АС установленного класса.

Для проверки регистрации изменения полномочий субъектов доступа необходимо произвести эти изменения при помощи средств СЗИ и просмотреть результаты регистрации.

Для проверки процедуры автоматического учета создаваемых, инициируемых защищаемых информационных ресурсов необходимо смоделировать создание (инициацию) защищаемого носителя информации на тех этапах технологического процесса, где используются СВТ.

При помощи средств СЗИ просматриваются результаты учета. Должны быть автоматически учтены все созданные (инициированные) защищаемые информационные ресурсы с требуемыми параметрами учета.

Проверяется ведение учета всех защищаемых носителей информации, осуществляемого вручную персоналом, путем проверки технологических инструкций, степени ознакомления с ними конкретных исполнителей, проверки правильности ведения карточек и журналов учета.

Проверка средств очистки (обнуления, обезличивания) освобождаемых областей оперативной и внешней памяти ЭВМ осуществляется путем записи в область памяти пользователем некоторой определенной информации, фиксирования конкретного физического адреса области, освобождения области данным пользователем, попытки считывания информации из данной области по зафиксированному адресу и сравнения считанного с первоначально записанной в эту область информацией. При нормальной работе средств очистки освобождаемых областей памяти ранее записанная информация должна отличаться от считанной.

Проверка средств сигнализации попыток нарушения защиты осуществляется путем моделирования несанкционированных обращений к защищаемым объектам доступа и отслеживания появления определенных сигналов в местах интерфейса с администратором системы защиты и нарушителем.

11) Испытания подсистемы обеспечения целостности.

Проверка подсистемы обеспечения целостности СЗИ от НСД проводится по перечню функций, определенных указанным РД Гостехкомиссии России для данного класса АС.

Надежность функций контроля целостности программных средств может быть проверена при помощи внесения изменений в отдельные программы или их подмены. При этом отслеживается реакция системы защиты на произведенные нарушения.

При проверке **обеспечения неизменности программной среды** определяется наличие и работоспособность технологии внесения новых программных средств в операционную среду, предусматривающую процедуры экспертной оценки или верификации новых программных средств для выявления потенциально опасных для СЗИ программных функций, критерии санкционирования ввода программ в операционную среду и допуска определенных категорий пользователей к этим программам.

Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду.

По результатам анализа технологического процесса обработки и хранения конфиденциальной информации в АС **проверяется выполнение требований по физической охране средств АС и носителей информации в АС,** пропускному режиму и оборудованию помещений необходимыми защитными средствами.

Проверяется наличие в системе администратора системы защиты информации, оценивается его уровень подготовленности и степень оснащения его рабочего места необходимыми средствами оперативного контроля и сопровождения СЗИ.

Проверяется наличие и работоспособность средств периодического тестирования всех функций СЗИ НСД, наличие графика проведения тестирования. Средства тестирования должны давать однозначную информацию о всех функциях СЗИ НСД, предусмотренных требованиями к данному классу АС.

Приводится выборочная проверка используемых в системе программных средств на наличие компьютерных вирусов.

Проверяется наличие и работоспособность технологии восстановления программных средств защиты информации в АС, ведения архива программных средств защиты, условия и периодичность их обновления и тестирования.

Автоматическое оперативное восстановление функций СЗИ НСД при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверки (тестирования) функций СЗИ НСД.

Если для данного класса АС требуется наличие сертифицированных средств защиты, **проверяется наличие таких сертификатов соответствия, а также установленные в них классы защищенности.**

12) Рекомендации по результатам испытаний.

Комиссия может рекомендовать следующие меры по устранению недостатков:

- применение дополнительных организационно-технических мероприятий по защите информации;
- доработка организационно-распорядительной документации;
- применение дополнительных сертифицированных средств защиты информации;
- исключение отдельных программных средств из состава АС. <1>

<1> Программа и методики проведения аттестационных испытаний объектов информатизации (URL: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BF%D0%BC%D0%B8).