Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

Кафедра защиты информации

А. М. Тимофеев

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ. ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ДЛЯ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рекомендовано УМО по образованию
в области информатики и радиоэлектроники
в качестве учебно-методического пособия для специальности
6-05-0611-02 «Информационная безопасность»

Минск БГУИР 2025

УДК 004.056.5:336.71(076)
ББК 32.972.5я73+65.262.1я73
Т41

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем учреждения образования
«Белорусская государственная академия связи»
(протокол № 9 от 09.04.2024);

заведующий кафедрой инфокоммуникационных технологий
учреждения образования «Белорусский государственный университет
информатики и радиоэлектроники»
доктор технических наук, профессор В. Ю. Цветков;

доцент кафедры информационно-измерительной техники и технологии
Белорусского национального технического университета
кандидат технических наук, доцент Н. Н. Ризноокая;

начальник испытательной лаборатории по требованиям
безопасности информации управления защиты информации
научно-производственного республиканского унитарного предприятия
«Научно-исследовательский институт технической
защиты информации» М. Л. Радюкевич

Тимофеев, А. М.

Т41 Защита информации в банковских технологиях. Требования к системам защиты для типовых информационных систем : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2025. – 120 с. : ил.

ISBN 978-985-543-804-6.

Содержит четыре практических занятия, направленных на изучение нормативных правовых актов Республики Беларусь в сфере защиты информации, включая особенности проектирования, создания и эксплуатации систем защиты информации. Композиционно каждое практическое занятие включает краткие теоретические сведения, практическое задание, содержание отчета и перечень контрольных вопросов. Для выполнения практических заданий используется специально разработанная компьютерная программа TAMbsuirCryptoLab. Законодательный материал дан по состоянию на 01.09.2024.

Предназначено для студентов всех форм обучения, может быть полезно магистрантам инфокоммуникационных специальностей, а также специалистам, работающим в области проектирования, создания и эксплуатации систем защиты информации.

УДК 004.056.5:336.71(076)
ББК 332.972.5я73+65.262.1я73

ISBN 978-985-543-804-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время информационные технологии продолжают достаточно интенсивно развиваться и находят применение в различных сферах, включая не только банковские информационные системы, но и другие (функционирующие в образовании, здравоохранении, сельском хозяйстве, связи и др.). В преобладающем большинстве случаев в отношении существующих, проектируемых или модернизируемых информационных систем требуется реализовывать определенные механизмы защиты информации [1–4]. Это может быть обусловлено следующими основными факторами:

– наличием отрытых каналов передачи данных, например, относящихся к сети Интернет, телефонной сети общего пользования и пр.;

– выполнением в информационных системах каких-либо юридически значимых действий, совершаемых с персональными данными, например, их сбор, систематизацию, хранение, изменение, использование, блокирование, распространение, предоставление, удаление и пр.;

– наличием или отсутствием информации, составляющей коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено;

– наличием или отсутствием в информационных системах служебной информации ограниченного распространения.

Под защитой информации будем понимать комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации.

В Республике Беларусь при реализации на практике тех или иных мер защиты информации чрезвычайно важно выполнять требования, установленные национальным законодательством, которые включают [5–10]:

– требования по обеспечению защиты данных;

– требования по обеспечению идентификации и аутентификации;

– требования по защите системы защиты информации информационной системы;

– обеспечение криптографической защиты информации;

– дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре;

– иные требования.

Выполнение указанных выше требований предусматривает:

– реализацию процедуры отнесения информационных систем к классам типовых;

– определение обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем;

– установление минимальных и достаточных наборов технических средств и организационных мер защиты информации с учетом применяемых технологий и типовых классов, к которым относятся информационные системы;

– изучение требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем.

Таким образом, при подготовке специалистов в области информационной безопасности представляется весьма важным изучение вопросов проектирования и создания систем защиты информации, а также эксплуатации информационных систем с применением систем защиты информации с учетом

соответствующих требований законодательства Республики Беларусь, что и является целью данного учебно-методического пособия.

Содержание учебно-методического пособия включает четыре темы практических занятий, направленных на изучение основных нормативно-правовых актов Республики Беларусь в области защиты информации применительно к типовым информационным системам, за исключением специфических средств защиты информации.

В результате выполнения практических заданий:

1) будут изучены:

– основные нормативно-правовые акты Республики Беларусь в области защиты информации;

– принципы категорирования обрабатываемой информации, используемые до проведения работ по проектированию систем защиты информации собственником (владельцем) информационной системы;

– обязательные и рекомендуемые требования, предъявляемые к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем и используемые в техническом задании на создание систем защиты информации;

2) будут получены практические навыки:

– отнесения информационных систем к классам типовых;

– определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы;

– установления каналов передачи данных, допустимых при организации взаимодействия информационных систем с учетом применяемых технологий и классов типовых информационных систем.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 1.
КЛАССЫ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Цель: изучение особенностей отнесения информационных систем к классам типовых и принципов категорирования обрабатываемой информации, используемых до проведения работ по проектированию системы защиты информации собственником (владельцем) информационной системы.

1.1 Краткие теоретические сведения

До проведения работ по проектированию системы защиты информации собственник (владелец) информационной системы осуществляет категорирование информации, которая будет обрабатываться в информационной системе, а также отнесение информационной системы к классу типовых информационных систем [6–10].

Вначале приведем основные используемые термины и определения [6; 9].

База данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях.

Банк данных – это организационно-техническая система, включающая одну или несколько баз данных и систему управления ими.

Биометрические персональные данные – это информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое).

Владелец информационных систем – это субъект информационных отношений, реализующий права владения, пользования и распоряжения

информационными системами в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь.

Владелец коммерческой тайны – это юридическое или физическое лицо, в том числе индивидуальный предприниматель, а также государственный орган, иностранная организация, не являющаяся юридическим лицом, правомерно обладающие сведениями, в отношении которых такими лицами в соответствии с Законом Республики Беларусь «О коммерческой тайне» [7] установлен режим коммерческой тайны, за исключением случаев, когда эти сведения составляют коммерческую тайну других лиц.

Генетические персональные данные – это информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца.

Государственная информационная система – это информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Государственный информационный ресурс – это информационный ресурс, формируемый или приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Документированная информация – это информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.

Доступ к информации – это возможность получения информации и пользования ею.

Доступ к информационной системе – это возможность использования информационной системы.

Доступ к коммерческой тайне – это возможность ознакомления с согласия владельца коммерческой тайны или на ином законном основании определенного круга лиц со сведениями, составляющими коммерческую тайну.

Защита информации – это комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации.

Информатизация – это организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений.

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная сеть – это совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи.

Информационная система – это совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационная технология – это совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Информационная услуга – это деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также защиты информации.

Информационные отношения – это отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Информационный посредник – это субъект информационных отношений, предоставляющий информационные услуги обладателям и (или) пользователям информации.

Информационный ресурс – это организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Коммерческая тайна – это сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям [7], в отношении которых установлен режим коммерческой тайны.

Комплекс программно-технических средств – это совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий.

Контрагент – это сторона гражданско-правового договора (за исключением лиц, состоящих в трудовых отношениях с владельцем коммерческой тайны), которой владелец коммерческой тайны предоставляет доступ к сведениям, составляющим коммерческую тайну.

Конфиденциальность информации – это требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь.

Носитель коммерческой тайны – это документ или иной материальный объект, на котором сведения, составляющие коммерческую тайну, содержатся в любой объективной форме, в том числе в виде символов, образов, сигналов, позволяющих эти сведения распознать и идентифицировать.

Обладатель информации – это субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору.

Обработка персональных данных – это любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

Общедоступные персональные данные – это персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов.

Обязательство о неразглашении коммерческой тайны – это гражданско-правовой договор, заключаемый владельцем коммерческой тайны или лицом, получившим к ней доступ, с лицом, состоящим в трудовых отношениях с владельцем коммерческой тайны или лицом, получившим к ней доступ, и определяющий обязательства сторон, связанные с соблюдением конфиденциальности сведений, составляющих коммерческую тайну.

Оператор информационной системы – это субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги.

Разглашение коммерческой тайны – это действия (бездействие), в результате которых сведения, составляющие коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без согласия владельца коммерческой тайны или иного законного основания.

Режим коммерческой тайны – это правовые, организационные, технические и иные меры, принимаемые в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

Персональные данные – это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Пользователь информации – это субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею.

Пользователь информационной системы – это субъект информационных отношений, получивший доступ к информационной системе и пользующийся ею.

Предоставление информации – это действия, направленные на ознакомление с информацией определенного круга лиц.

Предоставление персональных данных – это действия, направленные на ознакомление с персональными данными определенного лица или круга лиц.

Распространение информации – это действия, направленные на ознакомление с информацией неопределенного круга лиц.

Распространение персональных данных – это действия, направленные на ознакомление с персональными данными неопределенного круга лиц.

Собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – это субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями.

Соглашение о конфиденциальности – это гражданско-правовой договор, заключаемый владельцем коммерческой тайны с контрагентом, предметом которого являются обязательства сторон по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Специальные персональные данные – это персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные.

Субъект персональных данных – это физическое лицо, в отношении которого осуществляется обработка персональных данных.

Удаление персональных данных – это действия, в результате которых становится невозможным восстановить персональные данные в информационных ресурсах (системах), содержащих персональные данные, и (или) в результате которых уничтожаются материальные носители персональных данных.

Уполномоченное лицо – это государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах.

Физическое лицо, которое может быть идентифицировано, – это физическое лицо, которое может быть прямо или косвенно определено, в частности, через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Субъектами информационных отношений могут являться:

– Республика Беларусь, административно-территориальные единицы Республики Беларусь;

– государственные органы, другие государственные организации;

– иные юридические лица, организации, не являющиеся юридическими лицами;

– физические лица, в том числе индивидуальные предприниматели;

– иностранные государства, международные организации.

Субъекты информационных отношений могут выступать в качестве:

– обладателей информации;

– пользователей информации, информационных систем и (или) информационных сетей;

– собственников и владельцев программно-технических средств, информационных ресурсов, информационных систем и информационных сетей;

– информационных посредников;

– операторов информационных систем.

Далее рассмотрим принципы категорирования обрабатываемой информации, которая планируется к обработке в проектируемой информационной системе.

Категорирование информации выполняется в соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации» [9].

В зависимости от категории доступа информация делится на два вида:

– общедоступная информация;

– информация, распространение и (или) предоставление которой ограничено.

К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:

– о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;

– о деятельности государственных органов, общественных объединений;

– о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

– о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

– о состоянии преступности, а также о фактах нарушения законности;

– о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

– о размерах золотого запаса;

– об обобщенных показателях по внешней задолженности;

– о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

– накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

К информации, распространение и (или) предоставление которой ограничено, относится:

– информация о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– информация, составляющая коммерческую и профессиональную тайну;

– информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

Теперь рассмотрим основные особенности отнесения информационных систем к классам типовых.

Отнесение информационной системы к классу типовых информационных систем выполняется на основе данных, представленных в таблице 1.

Таблица 1 – Классы типовых информационных систем [10]

Класс	Характеристика информационной системы
1	2
1 класс 6-частн	Негосударственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных
2 класс 6-гос	Государственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных
3 класс 5-частн	Негосударственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных
4 класс 5-гос	Государственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных
5 класс 4-ин	Информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных
6 класс 4-спец	Информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных
7 класс 4-бг	Информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных
8 класс 4-юл	Информационные системы, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые не имеют подключений к открытым каналам передачи данных
9 класс 4-дсп	Информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных
10 класс 3-ин	Информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных
11 класс 3-спец	Информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных

Продолжение таблицы 1

1	2
12 класс 3-бг	Информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных
13 класс 3-юл	Информационные системы, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые подключены к открытым каналам передачи данных
14 класс 3-дсп	Информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных

В отношении информации о частной жизни физического лица и персональных данных в соответствии с законодательством Республики Беларусь определено следующее:

– никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь;

– сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь;

– порядок получения, передачи, сбора, обработки, накопления, хранения и предоставления информации о частной жизни физического лица и персональных данных, а также пользования ими устанавливается законодательными актами Республики Беларусь.

В соответствии с законодательством Республики Беларусь существуют общие требования в отношении обработки персональных данных:

– обработка персональных данных осуществляется в соответствии с Законом Республики Беларусь «О защите персональных данных» [6] и иными актами законодательства;

– обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц;

– обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом Республики Беларусь «О защите персональных данных» [6] и иными законодательными актами. В случае обработки персональных данных без согласия субъекта персональных данных цели обработки персональных данных устанавливаются Законом Республики Беларусь «О защите персональных данных» [6] и иными законодательными актами;

– обработка персональных данных должна ограничиваться достижением конкретных, заранее заявленных законных целей. Не допускается обработка персональных данных, не совместимая с первоначально заявленными целями их обработки. В случае необходимости изменения первоначально заявленных целей обработки персональных данных оператор обязан получить согласие субъекта персональных данных на обработку его персональных данных в соответствии с измененными целями обработки персональных данных при отсутствии иных оснований для такой обработки, предусмотренных Законом Республики Беларусь «О защите персональных данных» [6] и иными законодательными актами;

– содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям их обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

– обработка персональных данных должна носить прозрачный характер. В этих целях субъекту персональных данных в случаях, предусмотренных Законом Республики Беларусь «О защите персональных данных» [6], предоставляется соответствующая информация, касающаяся обработки его персональных данных;

– оператор обязан принимать меры по обеспечению достоверности обрабатываемых им персональных данных, при необходимости обновлять их;

– хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных.

Законодательство о коммерческой тайне основывается на Конституции Республики Беларусь и состоит из Гражданского кодекса Республики Беларусь, Закона Республики Беларусь «О коммерческой тайне» [7] и иных актов законодательства, а также международных договоров Республики Беларусь.

Если международным договором Республики Беларусь установлены иные правила, чем те, которые содержатся в Законе Республики Беларусь «О коммерческой тайне» [7], то применяются правила международного договора.

Сведения имеют коммерческую ценность в случае, если обладание ими позволяет лицу при существующих или возможных обстоятельствах увеличить доходы, сократить расходы, сохранить положение на рынке товаров, работ или услуг либо получить иную коммерческую выгоду.

Сведения, охраняемые в режиме коммерческой тайны. Режим коммерческой тайны может устанавливаться в отношении сведений, которые одновременно соответствуют следующим требованиям:

– не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями;

– имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам;

– не являются объектами исключительных прав на результаты интеллектуальной деятельности;

– не отнесены в установленном порядке к государственным секретам.

Правовая охрана коммерческой тайны возникает с момента установления в отношении сведений, указанных выше, режима коммерческой тайны и не прекращается до тех пор, пока охраняемые сведения соответствуют этим требованиям и действует установленный режим коммерческой тайны.

Реорганизация юридического лица, а также прекращение деятельности индивидуального предпринимателя не являются основанием для прекращения правовой охраны коммерческой тайны.

При ликвидации юридического лица собственник имущества (учредители, участники, другие уполномоченные в соответствии с законодательными актами лица) вправе решить вопрос о порядке дальнейшего сохранения и использования сведений, составляющих коммерческую тайну, и о последствиях принятия такого решения для лиц, получивших доступ к коммерческой тайне до ликвидации юридического лица.

Сведения, которые не могут составлять коммерческую тайну, включают:

– содержащиеся в учредительных документах юридического лица, а также внесенные в Единый государственный регистр юридических лиц и индивидуальных предпринимателей;

– содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

– являющиеся врачебной, адвокатской, банковской, налоговой или иной охраняемой законом тайной;

– о недвижимом имуществе, правах и ограничениях (обременениях) прав на недвижимое имущество, содержащиеся в едином государственном регистре недвижимого имущества, прав на него и сделок с ним;

– о составе имущества государственных юридических лиц и юридических лиц, акции (доли в уставных фондах) которых принадлежат государству;

– об использовании средств республиканского и (или) местных бюджетов;

– о состоянии окружающей среды, противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих или способных оказать негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и населения в целом;

– о подлежащих уплате суммах налогов, сборов (пошлин) и других обязательных платежей;

– о численности и составе работников, об условиях и охране труда, о показателях производственного травматизма и профессиональной заболеваемости, а также о наличии свободных рабочих мест (вакансий);

– о задолженности нанимателей по выплате заработной платы и по социальным выплатам;

– о нарушениях законодательства и фактах привлечения к ответственности за совершение этих нарушений;

– об условиях аукционов (конкурсов) по продаже объектов приватизации и конкурсов по передаче принадлежащих Республике Беларусь или ее административно-территориальной единице акций открытых акционерных обществ в доверительное управление, в том числе с правом выкупа части этих акций по результатам доверительного управления, а также о проданных объектах приватизации, об условиях их продажи и о покупателях;

– о финансовом состоянии лица, предоставляемые в соответствии с требованиями законодательства об экономической несостоятельности (банкротстве);

– иные сведения, определенные законодательными актами.

Режим коммерческой тайны включает в себя следующие меры:

– ограничение доступа к коммерческой тайне путем установления порядка обращения с носителями коммерческой тайны, а также контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к коммерческой тайне;

– регулирование отношений, связанных с доступом работников к коммерческой тайне, на основании трудового договора (контракта), а также на основании обязательства о неразглашении коммерческой тайны, дополнительно заключаемого по требованию нанимателя с работником, получающим доступ к коммерческой тайне;

– регулирование отношений, связанных с доступом контрагентов к коммерческой тайне, на основании гражданско-правового договора;

– определение работников, ответственных за принятие мер по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Наряду с мерами, указанными выше, владелец коммерческой тайны вправе применять не запрещенные законодательством технические средства и методы защиты информации, а также другие меры, не противоречащие законодательству.

Работник имеет право обжаловать в судебном порядке принятие или изменение нанимателем отдельных мер по обеспечению конфиденциальности сведений, составляющих коммерческую тайну, ограничивающих его права.

Владелец коммерческой тайны может на носителях коммерческой тайны применять гриф «Коммерческая тайна» с указанием владельца коммерческой тайны (для юридических лиц – полное наименование и место нахождения, для физических лиц – фамилия, собственное имя, отчество (если таковое имеется) гражданина и место его жительства).

Владелец коммерческой тайны имеет право, не нарушая обязательств, принятых по заключенным им договорам, изменять или отменять режим коммерческой тайны, в том числе в отношении отдельных сведений, составляющих коммерческую тайну.

Если иное не определено соглашением сторон, владелец коммерческой тайны в срок, определенный гражданско-правовым договором с контрагентом, обязательством о неразглашении коммерческой тайны, обязан в письменной форме уведомить контрагентов, работников, в том числе бывших работников, в отношении которых действует обязательство о неразглашении коммерческой тайны, о затрагивающих их права и законные интересы изменении или отмене режима коммерческой тайны в целом либо в отношении отдельных сведений, составляющих коммерческую тайну.

Владелец коммерческой тайны вправе:

– изменять или отменять режим коммерческой тайны;

– изменять состав сведений, составляющих коммерческую тайну;

– использовать сведения, составляющие коммерческую тайну;

– разрешать или запрещать доступ других лиц к коммерческой тайне, изменять порядок и условия доступа к ней, если иное не установлено в Законе Республики Беларусь «О коммерческой тайне» [7] и иными законодательными актами;

– распоряжаться сведениями, составляющими коммерческую тайну;

– применять предусмотренные гражданским законодательством способы защиты от действий (бездействия) лиц, нарушающих режим коммерческой тайны или создающих угрозу такого нарушения.

Владелец коммерческой тайны может передать все или часть сведений, составляющих коммерческую тайну, другому лицу по договору, обязательным условием которого является обеспечение конфиденциальности передаваемых сведений.

Владелец коммерческой тайны обязан поддерживать установленный им режим коммерческой тайны, принимать меры, необходимые и достаточные для обеспечения конфиденциальности сведений, составляющих коммерческую тайну. ***Для выполнения этих обязанностей владелец коммерческой тайны вправе:***

– требовать от лиц, в том числе от государственных органов, получивших доступ к коммерческой тайне, исполнения предусмотренных в Законе Республики Беларусь «О коммерческой тайне» [7] и (или) договором обязательств по соблюдению конфиденциальности сведений, составляющих коммерческую тайну;

– требовать от лиц, получивших возможность ознакомления со сведениями, составляющими коммерческую тайну, в результате случайности либо действий других лиц, которые не имели права предоставлять доступ к коммерческой тайне, соблюдения конфиденциальности этих сведений;

– совершать иные действия для обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

Государственные органы и иные лица, получившие в соответствии с их требованием доступ к коммерческой тайне, обязаны создать условия, обеспечивающие соблюдение конфиденциальности сведений, составляющих коммерческую тайну.

Носители коммерческой тайны, предоставляемые по требованию государственных органов и иных лиц, должны быть идентифицированы владельцем коммерческой тайны путем нанесения грифа «Коммерческая тайна» с указанием ее владельца (для юридических лиц – полное наименование и место нахождения, для физических лиц – фамилия, собственное имя, отчество (если таковое имеется) гражданина и место его жительства).

Должностные лица государственных органов, а также работники иных лиц не вправе разглашать сведения, составляющие коммерческую тайну, или предоставлять доступ третьим лицам к сведениям, ставшим известными им в силу выполнения трудовых (служебных) обязанностей и составляющим коммерческую тайну, за исключением случаев, предусмотренных законодательными актами, а также не вправе использовать эти сведения в целях, непосредственно не связанных с выполнением трудовых (служебных) обязанностей.

В целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну, государственные органы и иные лица могут использовать любые не противоречащие законодательству способы ограничения доступа к таким сведениям.

Ознакомление участников уголовного, гражданского, хозяйственного, административного судопроизводства с содержащимися в материалах дела сведениями, составляющими коммерческую тайну, допускается только в части, относящейся непосредственно к существу дела, по судебному постановлению с возложением на них обязанности последующего сохранения конфиденциальности полученных сведений.

В соответствии с законодательством Республики Беларусь [8] к служебной информации ограниченного распространения относят сведения, перечень которых представлен в приложении А.

На документах (приложениях к документам), содержащих служебную информацию ограниченного распространения, а также их проектах и сопроводительных письмах к ним проставляется ограничительный гриф «Для служебного пользования».

Ограничительный гриф «Для служебного пользования» не проставляется на документах, содержащих общедоступную информацию, представленную выше.

При оформлении документа (приложения к документу), содержащего служебную информацию ограниченного распространения, ограничительный гриф «Для служебного пользования» и номер экземпляра проставляются в правом верхнем углу первого листа документа (приложения к документу), а также на первом листе сопроводительного письма к документу (при его составлении). При оформлении ограничительного грифа «Для служебного пользования» на компьютере применяется гарнитура шрифта Times New Roman (Times New Roman Cyr) в обычном начертании, размер шрифта не менее 12 пт.

Вопросы ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения, в том числе

подготовка и оформление проектов документов, содержащих служебную информацию ограниченного распространения, их регистрация, отправка, тиражирование, передача, ознакомление, контроль исполнения, хранение, уничтожение, использование, подготовка к передаче в архив государственного органа, юридического лица, не урегулированные Постановлением Совета Министров Республики Беларусь «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну» [8] и актами законодательства в сфере архивного дела и делопроизводства, регулируются локальными нормативными правовыми актами.

Должностные лица, принявшие решение об отнесении сведений к служебной информации ограниченного распространения и проставлении на документе, содержащем такие сведения, ограничительного грифа «Для служебного пользования», несут персональную ответственность за обоснованность принятого решения.

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами (носителями информации), содержащими такую информацию, работник государственного органа, юридического лица несет ответственность в соответствии с законодательством.

Отнесение информационной системы к классу типовых информационных систем оформляется актом по форме согласно приложению Б. Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) информационных систем, в которых обрабатываются персональные данные, составляют акт отнесения информационной системы к классу типовых информационных систем в произвольной форме.

1.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCriptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCriptoLab.exe» активируется программное обеспечение, и появится окно выбора задания для выполнения, показанное на рисунке 1.

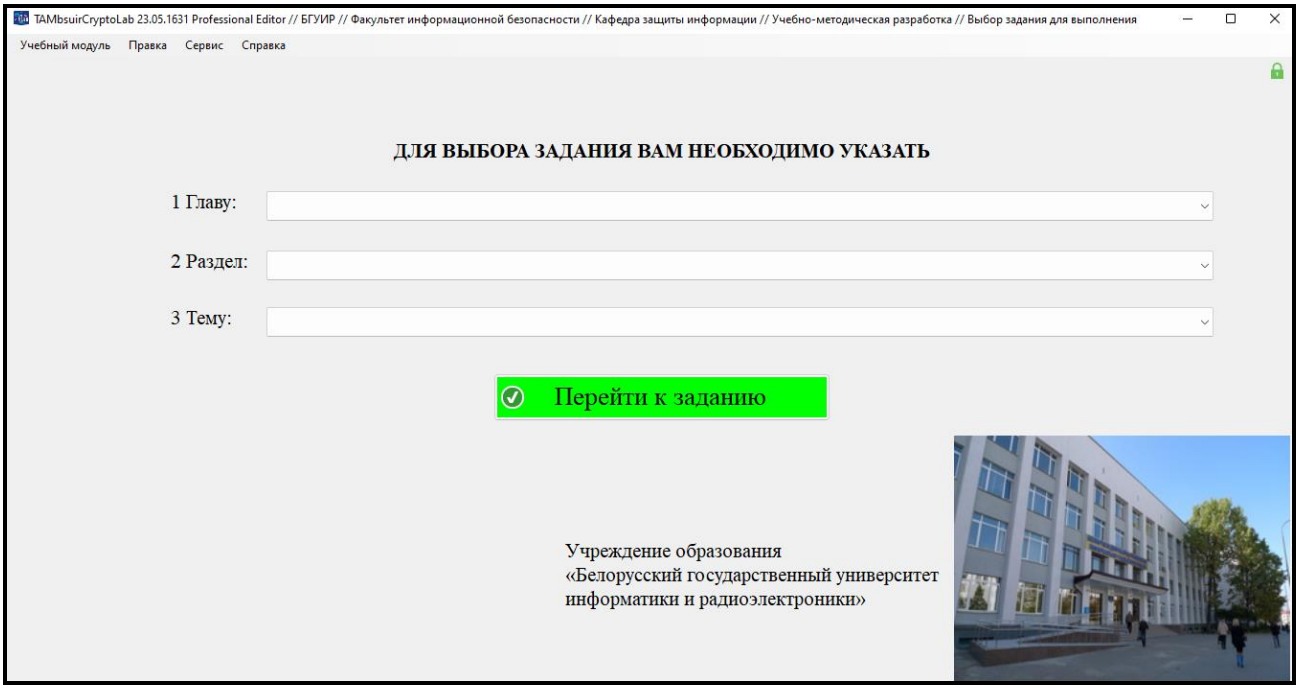


Рисунок 1 – Окно выбора задания

В верней области окна программы (см. рисунок 1) имеется графическое главное меню с четырьмя вкладками: «Учебный модуль», «Правка», «Сервис» и «Справка». Выбор элемента главного меню приводит к вызову появляющегося под ним подменю, некоторые из них, в свою очередь, также содержат подменю. Для удобства элементы подменю визуально объединены при помощи разделителей и имеют пиктограммы, иллюстрирующие опции программы. Выбор элемента главного меню, как и элемента подменю, осуществляется либо щелчком кнопки мыши, либо нажатием сочетания клавиш.

Вкладки «Учебный модуль» и «Справка» содержат набор подменю и дают возможность всем допущенным к выполнению задания пользователям воспользоваться дополнительными опциями программы (на любом этапе выполнения задания). Например, с помощью этих вкладок доступны такие опции программы, как ознакомление с методическими указаниями, изучение применяемых схем и расчетных формул, а также отмена загруженного учебного модуля и завершение его выполнения. В приложении В поясняется выбор опции программы через главное меню и с помощью сочетания клавиш (таблица В.1).

Остальные подменю, содержащиеся во вкладках «Учебный модуль» и «Справка», а также все подменю, имеющиеся во вкладках «Правка» и «Сервис», для выполнения задания не используются. Они применяются для реализации ряда вспомогательных функций и доступны только для преподавателя дисциплины, обладающего правами администратора.

В центральной области окна выбора задания (см. рисунок 1) имеется перечень из трех пунктов: «1 Главу:», «2 Раздел:» и «3 Тему:». Рядом с каждым из этих пунктов расположен выпадающий (раскрывающийся) список в виде элемента графического интерфейса (виджета), который позволяет осуществить выбор задания путем нажатия либо на сам виджет, либо на значок выпадающего списка, обозначенный треугольником.

В случае недопустимого, неправильного или некорректного заполнения предлагаемых полей программа генерирует сообщения об ошибках, в которых указывается их внутренний код, а также краткая информация о причине их возникновения. В приложении Г представлены сведения о возможных сообщениях об ошибках, включая их внутренние коды, возможные причины возникновения, действия, необходимые для их устранения (таблица Г.1), и примеры таких сообщений (рисунок Г.1).

Также в процессе выполнения задания программа может генерировать сообщения информационного характера, которые не имеют внутренних кодов и предназначены для дополнительного разъяснения специфики выполнения

отдельных этапов задания. На рисунке Г.2 в качестве примера приведено информационное сообщение, появляющееся при попытке выбора задания пользователем, у которого отсутствует допуск к его выполнению.

Для отмены выбранного задания и (или) введенных данных можно воспользоваться либо комбинацией клавиш Ctrl + J, либо подменю «Отменить загруженный блок и выбрать…», содержащимся во вкладке «Учебный модуль» главного меню программы (доступно на любом этапе выполнения задания). В результате на экране появится окно подтверждения, предотвращающее непреднамеренную отмену выбранного задания и введенных данных (рисунок Г.3). При нажатии кнопки «Да» выполнение текущего учебного модуля завершается, все данные, введенные ранее, при этом будут отменены, а на экране появится окно выбора задания (см. рисунок 1). Для возврата в окно выполнения задания и продолжения выполнения текущего учебного модуля без сброса введенных ранее данных в окне подтверждения необходимо нажать кнопку «Нет».

2 Выберите задание «Классы типовых информационных систем» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Главу:» – «ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ»;

2) пункт «2 Раздел:» – «ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ»;

3) пункт «3 Тему:» – «КЛАССЫ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению особенностей отнесения информационных систем к классам типовых и принципов категорирования обрабатываемой информации, используемых до проведения

работ по проектированию системы защиты информации собственником (владельцем) информационной системы, показанное на рисунке 2.

Рисунок 2 – Общий план выполнения задания по изучению особенностей отнесения информационных систем к классам типовых

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по составлению и оформлению заявлений о выдаче лицензий на право осуществления деятельности в области защиты информации.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 2) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 3, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

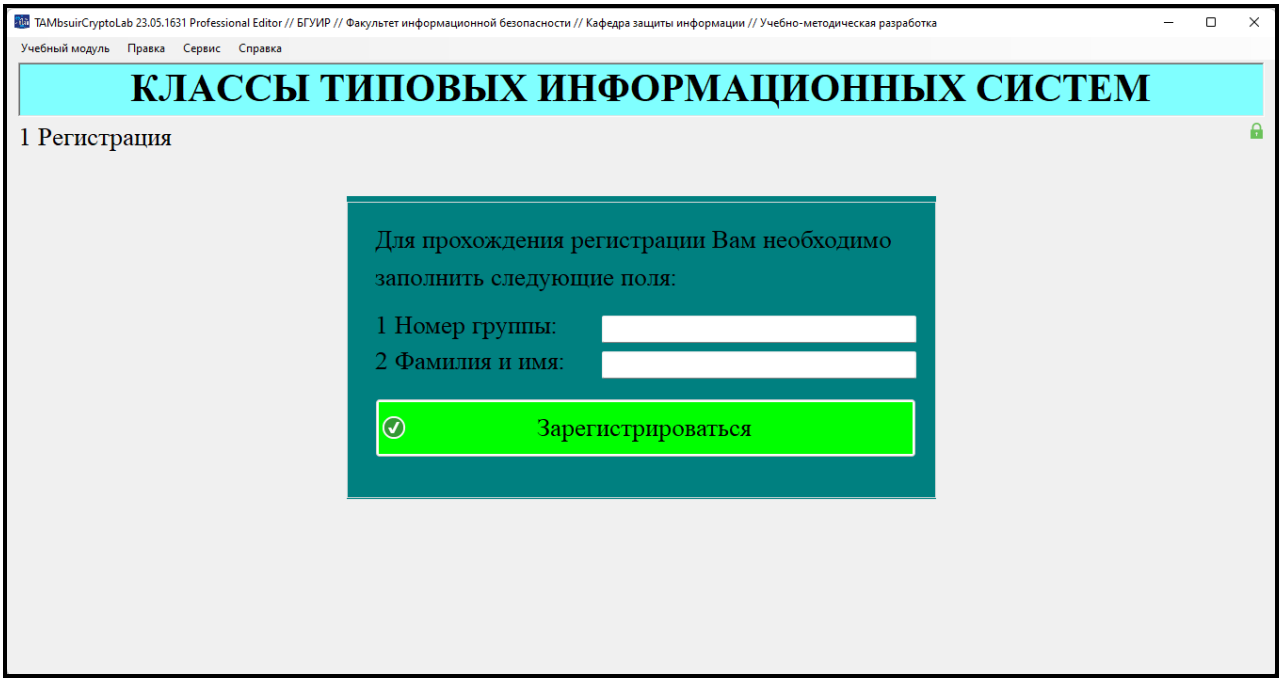


Рисунок 3 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению особенностей отнесения информационных систем к классам типовых

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 4.

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (рисунок 4) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 5, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

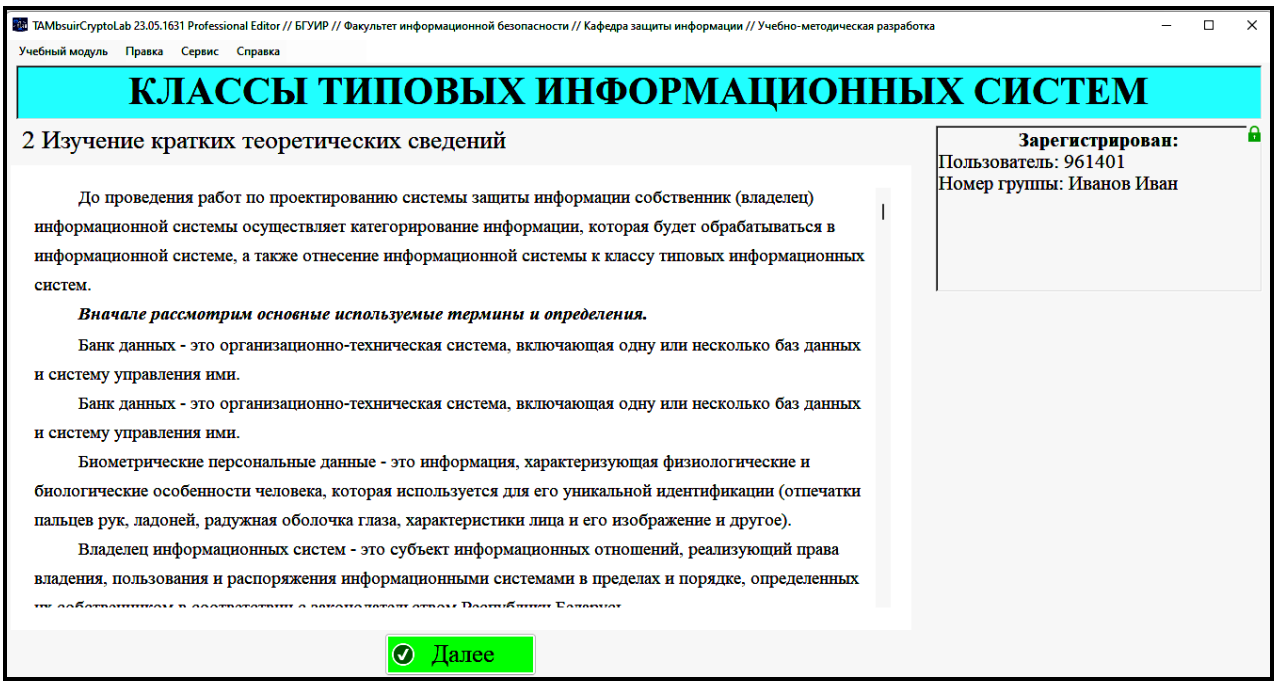


Рисунок 4 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению особенностей отнесения информационных систем к классам типовых

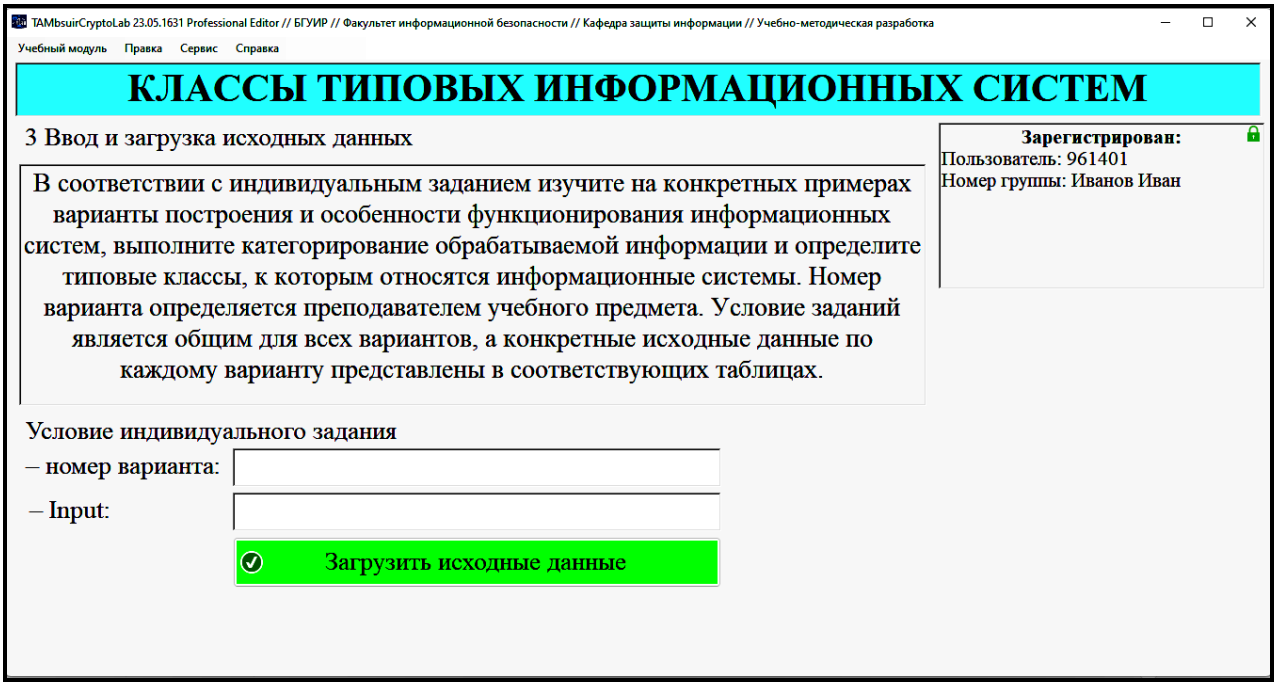


Рисунок 5 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению особенностей отнесения информационных систем к классам типовых

В результате на экране появится окно для изучения различных вариантов построения и особенностей функционирования информационных систем, соответствующее этапу 4 общего плана задания, показанное на рисунке 6.

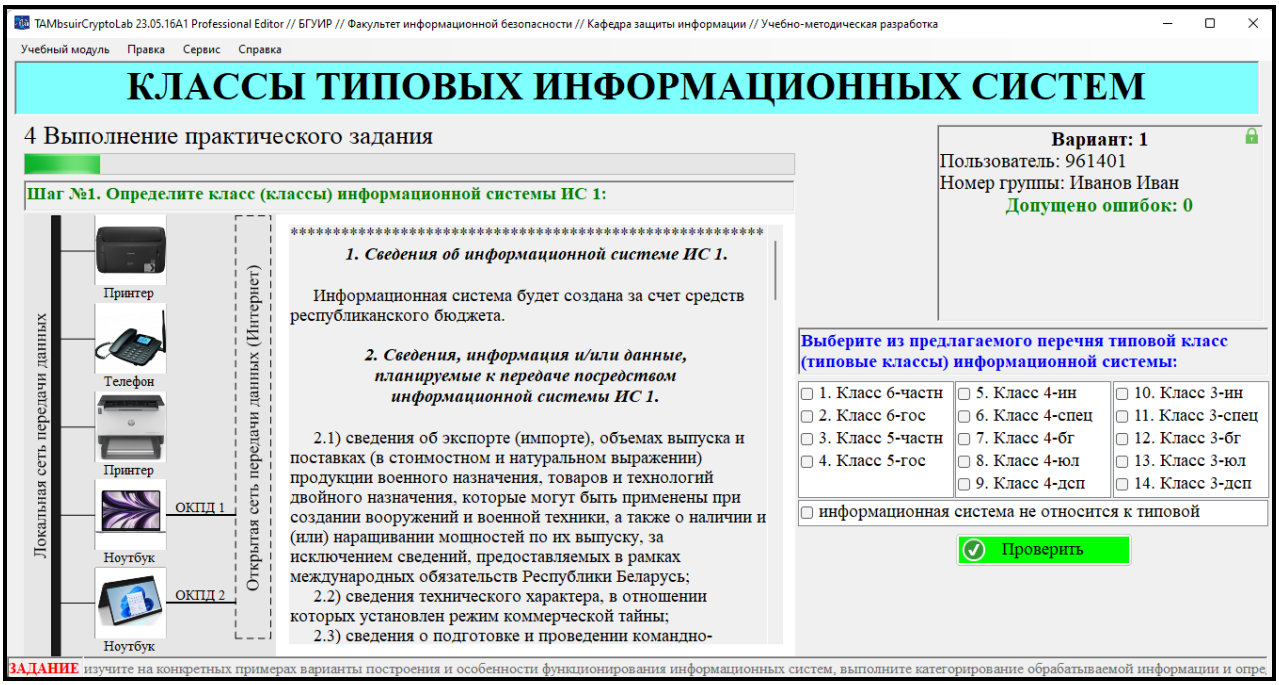


Рисунок 6 – Внешний вид окна для изучения особенностей отнесения информационных систем к классам типовых

5 Выполните предлагаемые задания по изучению различных вариантов построения и функционирования информационных систем, влияющих на процедуру отнесения информационных систем к классам типовых.

Номер варианта задания определяется преподавателем дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 6, и заключается в пошаговом исследовании различных вариантов построения и функционирования информационных систем, влияющих на процедуру отнесения информационных систем к классам типовых, представленных в

левой центральной области окна. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде бегущей строки.

Суть выполнения каждого шага задания заключается в изучении предлагаемого варианта построения информационной системы, оценке особенностей ее функционирования с учетом требований законодательства Республики Беларусь в сфере защиты информации, проведении категорирования обрабатываемой информации и определении на основании этого типового класса (типовых классов), к которому (которым) относится информационная система, путем выбора соответствующих пунктов (см. рисунок 6, нижнюю правую область окна с подзаголовком «Выберите из предлагаемого перечня типовой класс (типовые классы) информационной системы:»).

Чтобы выбрать пункт, необходимо нажать на него, после чего он будет отмечен галочкой; при повторном нажатии выбор пункта отменяется, и галочка снимается. Галочки необходимо установить рядом с теми пунктами, которые соответствуют предлагаемому варианту информационной системы.

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если один или несколько пунктов выбран (выбраны) неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне изучения особенностей отнесения информационных систем к классам типовых (см. рисунок 6).

Задание по изучению различных вариантов построения и функционирования информационных систем, влияющих на процедуру отнесения информационных систем к классам типовых, считается выполненным, если все шаги завершены успешно.

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю дисциплины.

Задание считается выполненным, если пункты 1–6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 7, *а*.

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 7, *б*. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш Ctrl + J, в появившемся окне (рисунок Г.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2–7 практического задания.

1.3 Содержание отчета

1 Цель практического занятия.

2 Краткие теоретические сведения об особенностях отнесения информационных систем к классам типовых.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

а

б

а – задание выполнено; *б* – задание не выполнено

Рисунок 7 – Заключительные результаты выполнения задания по изучению особенностей отнесения информационных систем к классам типовых

1.4 Контрольные вопросы

1 Для чего используется процедура отнесения информационных систем к классам типовых?

2 Какие существуют виды информации в зависимости от категории доступа?

3 Какие существуют требования в отношении обработки персональных данных?

4 При каких условиях в отношении некоторых сведений может быть установлен режим коммерческой тайны?

5 Какая информация относится к служебной информации ограниченного распространения в области банковской деятельности?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 2.
ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Цель: изучение обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем и используемых в техническом задании на создание систем защиты информации.

2.1 Краткие теоретические сведения

На этапе проектирования системы защиты информации осуществляются [10]:

– анализ структуры информационной системы и информационных потоков (внутренних и внешних) в целях определения состава (количества) и мест размещения элементов информационной системы (аппаратных и программных), ее физических и логических границ;

– издание политики информационной безопасности. При этом физическое лицо, являющееся собственником (владельцем) информационной системы, в которой обрабатываются персональные данные, за исключением индивидуального предпринимателя, вправе не издавать политику информационной безопасности;

– определение требований к системе защиты информации в техническом задании на создание системы защиты информации;

– выбор средств технической и криптографической защиты информации;

– разработка (корректировка) общей схемы системы защиты информации.

Политика информационной безопасности должна содержать следующее:

– цели и принципы защиты информации;

– перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем (см. практическое занятие 1), перечень средств вычислительной техники, а также сведения о подразделении защиты информации или ином подразделении (должностном лице), ответственном за обеспечение защиты информации, если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами;

– обязанности пользователей информационной системы;

– порядок взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия), в том числе при осуществлении информационных отношений на правах операторов, посредников, пользователей информационных систем и обладателей информации.

Техническое задание разрабатывается собственником (владельцем) информационной системы либо специализированной организацией и утверждается собственником (владельцем) информационной системы.

Техническое задание должно содержать:

– наименование информационной системы с указанием присвоенного ей класса типовых информационных систем;

– требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно данным из таблицы Д.1 (приложение Д);

– сведения об организации взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия) с учетом требований согласно таблице Е.1 (приложение Е);

– порядок обезличивания персональных данных согласно приложению Ж (в случае их обработки в информационной системе);

– требования из числа реализованных в аттестованной в установленном порядке системе защиты информации информационной системы другого

собственника (владельца) – если функционирование информационной системы, для которой осуществляется проектирование системы защиты информации, предполагается на базе информационной системы другого собственника (владельца) в соответствии с требованиями из Приказа Оперативно-аналитического центра при Президенте Республики Беларусь «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [10];

– требования к средствам криптографической защиты информации, включая требования к криптографическим алгоритмам в зависимости от задач безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита), криптографическим протоколам, управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям безопасности и форматам данных. Профили требований, предъявляемых к средствам криптографической защиты информации, определяются Оперативно-аналитическим центром при Президенте Республики Беларусь (ОАЦ);

– перечень документации на систему защиты информации.

Собственник (владелец) информационной системы вправе не включать в техническое задание отдельные обязательные требования к системе защиты информации при отсутствии в информационной системе соответствующего объекта (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер.

Общая схема системы защиты информации должна содержать:

– наименование информационной системы;

– класс типовых информационных систем;

– места размещения объектов информационной системы (ОИС): средств вычислительной техники, сетевого оборудования, системного и прикладного программного обеспечения, средств технической и криптографической защиты информации;

– физические границы информационной системы;

– внешние и внутренние информационные потоки и протоколы обмена защищаемой информацией.

В случае документирования создания информационных систем в соответствии с техническими нормативными правовыми актами, регламентирующими порядок создания автоматизированных систем, сведения, включенные в общую схему системы, могут быть предусмотрены в документах на автоматизированную информационную систему.

Допускается создание единой системы защиты информации:

– для нескольких информационных систем, функционирующих в общей программно-технической среде и принадлежащих одному собственнику (владельцу);

– нескольких типовых информационных систем, принадлежащих одному собственнику (владельцу).

При проектировании системы защиты информации информационной системы, функционирование которой предполагается на базе информационной системы другого собственника (владельца), имеющей аттестованную систему защиты информации, может быть предусмотрено применение требований, реализованных в системе защиты информации информационной системы этого собственника (владельца). Такие требования применяются в соответствии с договором на оказание соответствующих услуг.

2.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCriptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCriptoLab.exe» активируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «Требования к системам защиты информации для типовых информационных систем» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Главу:» – «ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ»;

2) пункт «2 Раздел:» – «ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ»;

3) пункт «3 Тему:» – «ТРЕБОВАНИЯ К СИСТЕМАМ ЗИ ДЛЯ ТИС».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем, показанное на рисунке 8.

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по изучению обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 8) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 9, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 10.

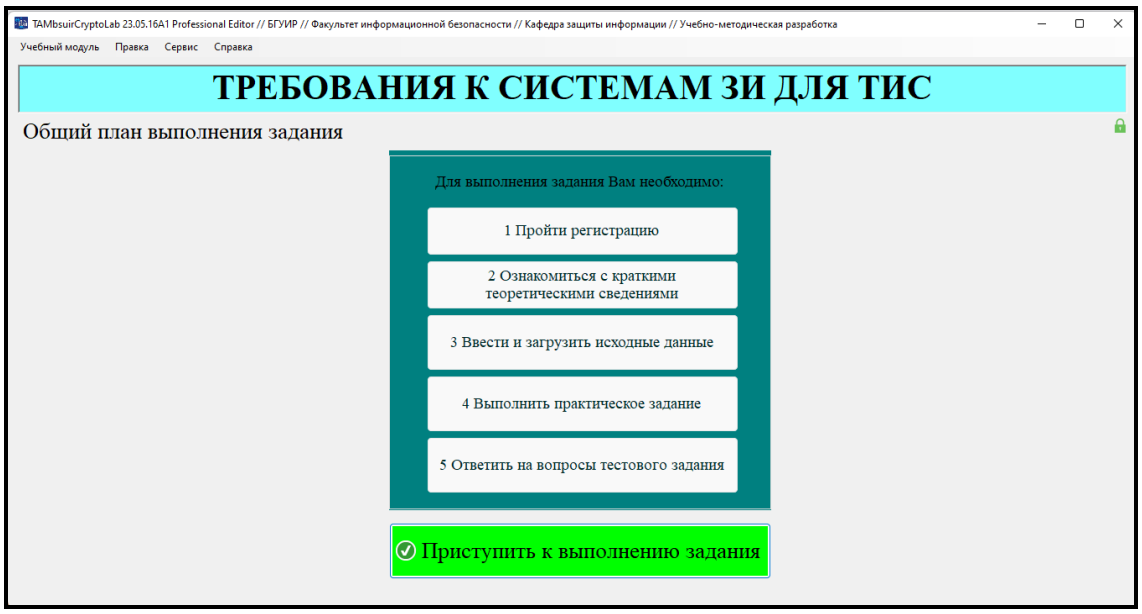


Рисунок 8 – Общий план выполнения задания по изучению обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем

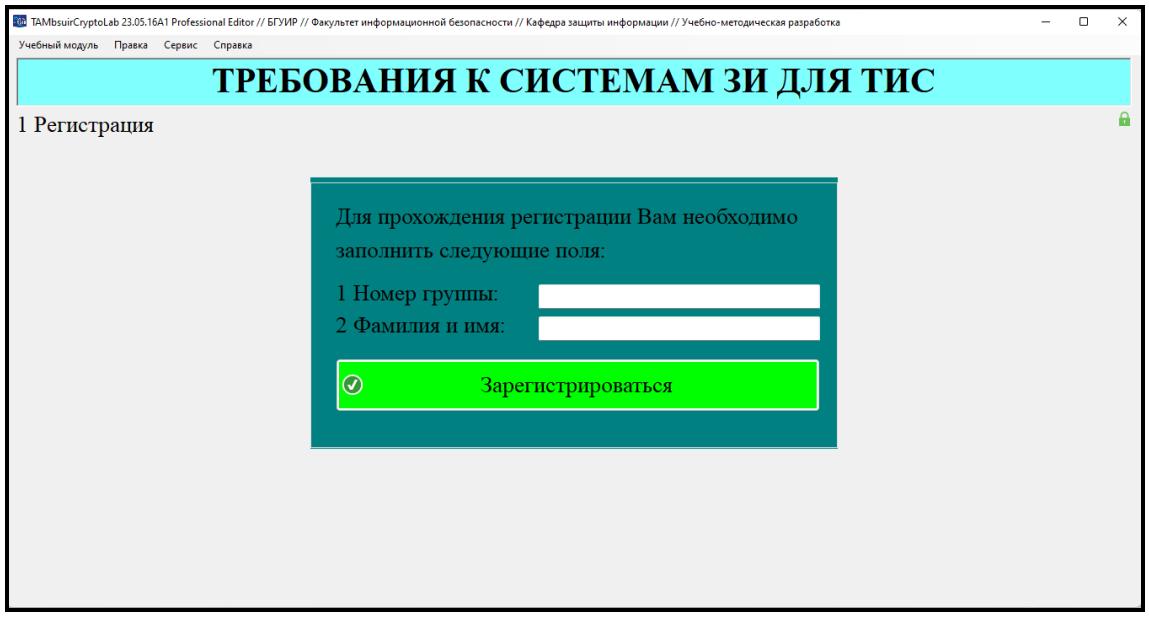


Рисунок 9 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем

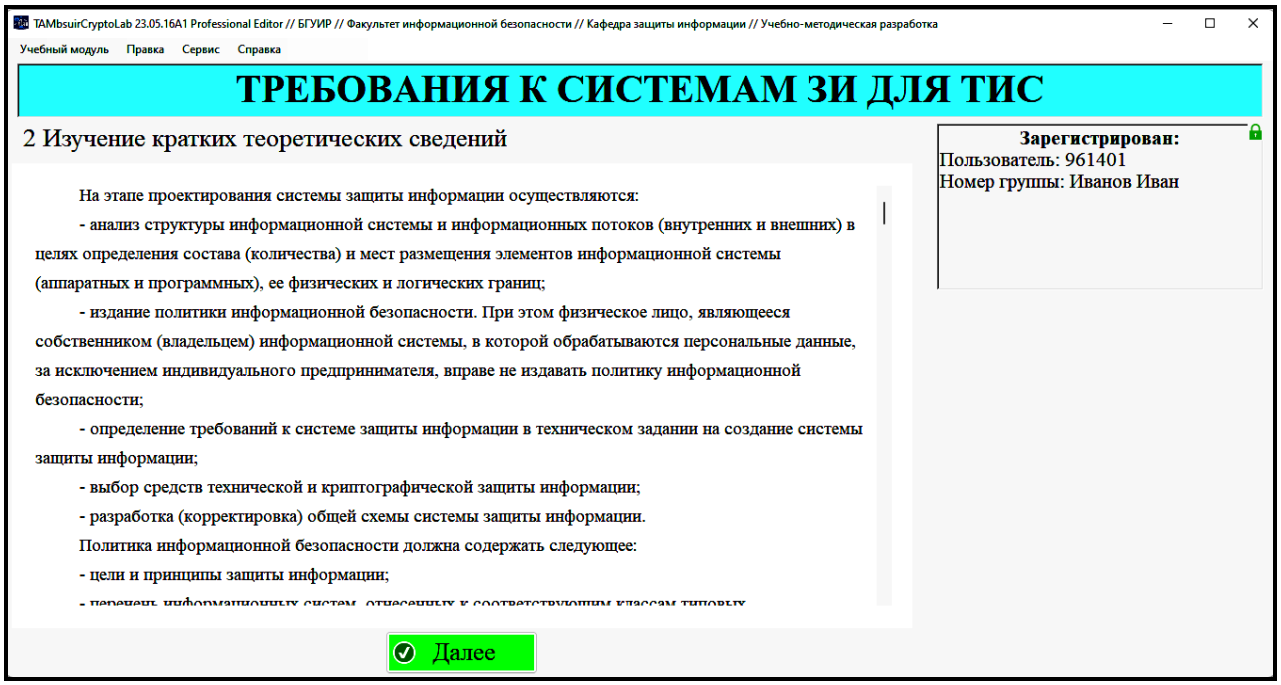


Рисунок 10 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 10) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 11, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

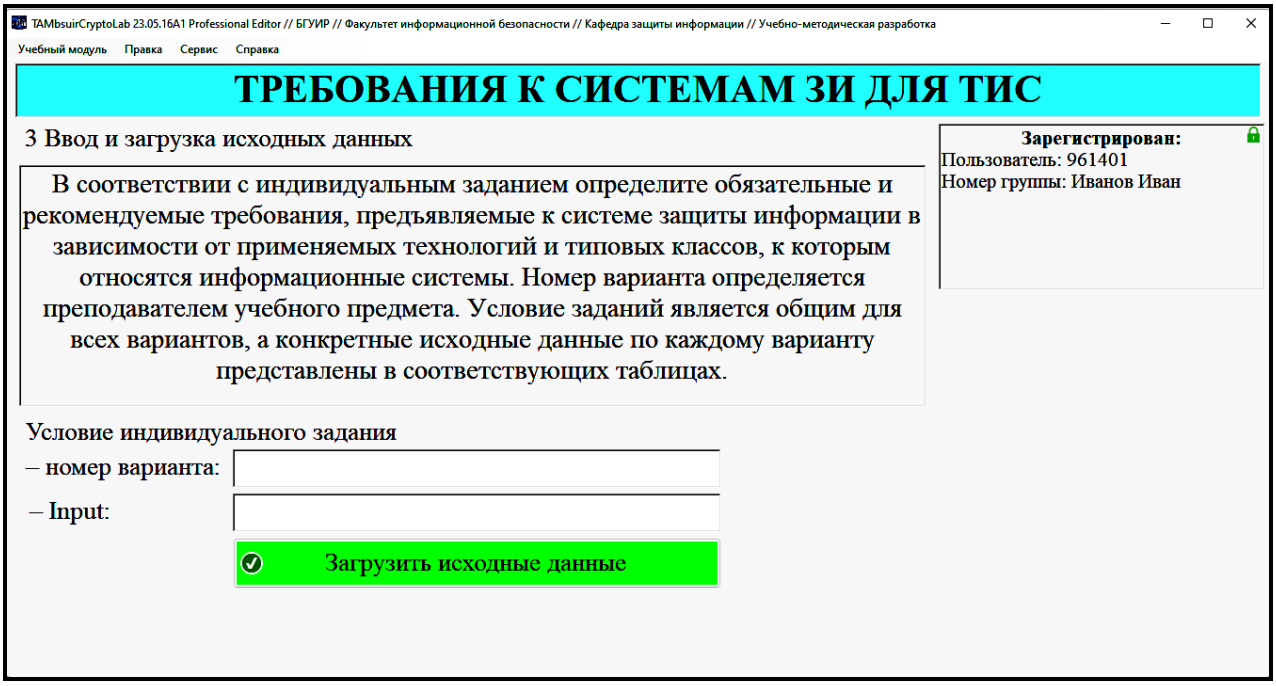


Рисунок 11 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению обязательных и рекомендуемых требований, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем

В результате на экране появится окно, соответствующее этапу 4 общего плана задания (рисунок 12) по определению обязательных и рекомендуемых требований, предъявляемых к системе защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы.

5 Выполните предлагаемые задания по определению обязательных и рекомендуемых требований, предъявляемых к системе защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы.

Номер варианта задания определяется преподавателем дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

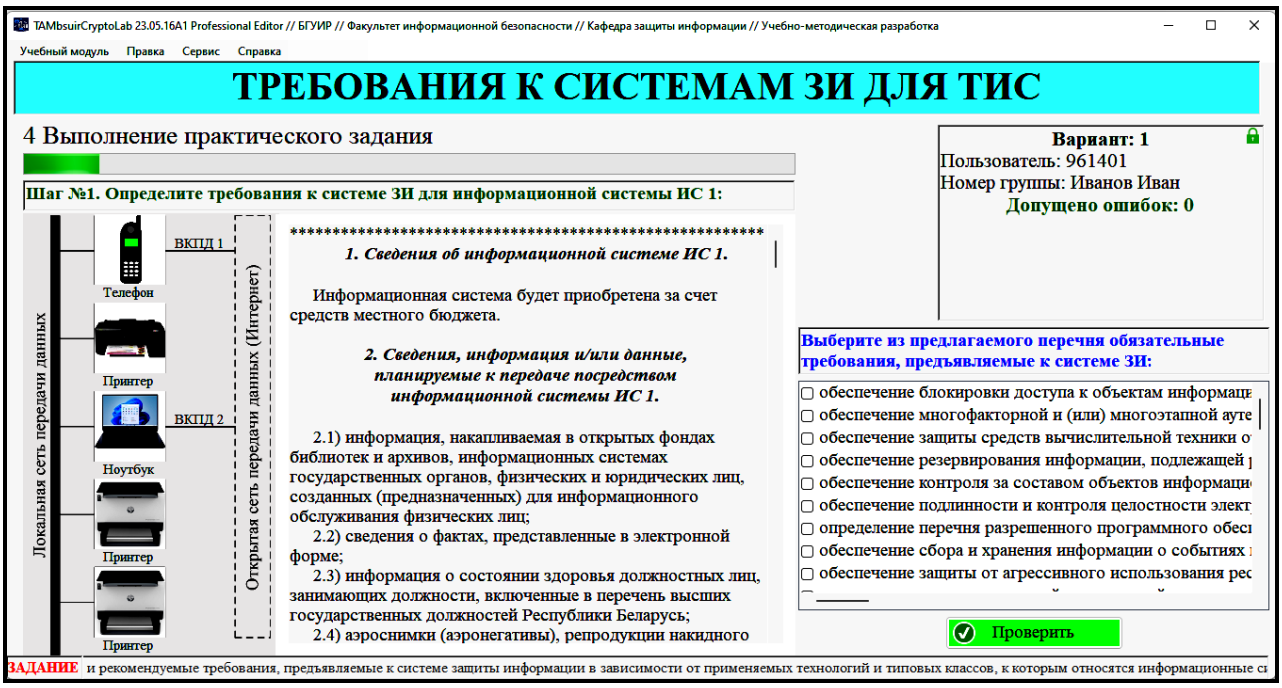


Рисунок 12 – Внешний вид окна по определению обязательных и рекомендуемых требований, предъявляемых к системе защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

Задание выполняется в окне, представленном на рисунке 12, и заключается в пошаговом определении обязательных и рекомендуемых требований, предъявляемых к системе защиты информации с учетом применяемых технологий и типовых классов, к которым относятся информационные системы. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде бегущей строки.

Суть выполнения каждого шага задания заключается в изучении предлагаемого варианта построения информационной системы, оценке ее типового класса (типовых классов) и определении на основании этого обязательных и рекомендуемых требований, предъявляемых к системе защиты информации путем выбора соответствующих пунктов (см. рисунок 12, нижнюю правую область окна с подзаголовком «Выберите из предлагаемого перечня обязательные требования, предъявляемые к системе ЗИ:»).

Чтобы выбрать пункт, необходимо нажать на него, после чего он будет отмечен галочкой; при повторном нажатии выбор пункта отменяется, и галочка снимается. Галочки необходимо установить рядом с теми пунктами, которые соответствуют предлагаемому варианту информационной системы.

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если один или несколько пунктов выбран (выбраны) неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне определения обязательных и рекомендуемых требований, предъявляемых к системе защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы (см. рисунок 12).

Задание по определению обязательных и рекомендуемых требований, предъявляемых к системе защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы, считается выполненным, если все шаги завершены успешно.

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю дисциплины.

Задание считается выполненным, если пункты 1–6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 13, *а*.

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 13, *б*. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш Ctrl + J, в появившемся окне (рисунок Г.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2–7 практического задания.

2.3 Содержание отчета

1 Цель практического занятия.

2 Краткие теоретические сведения о требованиях, предъявляемых к системам защиты информации в зависимости от применяемых технологий и классов типовых информационных систем и используемых в техническом задании на создание систем защиты информации.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

а

б

а – задание выполнено; *б* – задание не выполнено

Рисунок 13 – Заключительные результаты выполнения задания по определению обязательных и рекомендуемых требований, предъявляемых к системе защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

2.4 Контрольные вопросы

1 В чем отличия обязательных и рекомендуемых требований, предъявляемых к системам защиты информации, которые указывают в техническом задании на создание систем защиты информации?

2 Каким образом определяют рекомендуемые требования, предъявляемые к системам защиты информации, если информационная система относится только к одному типовому классу?

3 К какому наибольшему количеству типовых классов одновременно может относиться одна и та же информационная система, для которой необходимо определить обязательные требования, предъявляемые к системе защиты информации и используемые в техническом задании на ее создание?

4 Как определяют обязательные требования, предъявляемые к системам защиты информации, если информационная система одновременно относится к двум и более типовым классам?

5 Влияет ли структура информационной системы, ее физические и логические границы, а также содержание информационных потоков (внутренних и внешних) на состав и содержание требований, предъявляемых к системам защиты информации и используемых в техническом задании на создание систем защиты информации? Если да, то каким образом?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 3.
ВЫБОР ТЕХНИЧЕСКИХ СРЕДСТВ И ОРГАНИЗАЦИОННЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Цель: изучение методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы.

3.1 Краткие теоретические сведения

Вначале приведем основные термины и определения, используемые при выборе средств защиты информации [11–17].

Средства защиты информации – средства защиты государственных секретов, средства криптографической защиты информации, средства технической защиты информации.

Средства защиты государственных секретов – технические, программные, криптографические и другие средства, используемые для защиты государственных секретов, а также средства контроля эффективности защиты государственных секретов.

Средства криптографической защиты информации – программные, программно-аппаратные средства, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности.

Средства технической защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации

от несанкционированного доступа и несанкционированных воздействий на нее, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности.

Используемые технические средства и организационные меры защиты информации направлены на выполнение требований в области информационной безопасности в соответствии с перечнем, указанным в приложении Д.

Организационные меры защиты информации приведены в таблице 2.

Таблица 2 – Перечень обязательных и рекомендуемых организационных требований к системе защиты информации, подлежащих включению в техническое задание на создание системы защиты информации [10]

Наименование требования	Типовой класс информационной системы										Под-пункт [10]
	5	6	7	8	9	10	11	12	13	14	
1	2	3	4	5	6	7	8	9	10	11	12
Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности, информация о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации и другое)	+	+	+	+	+	+	+	+	+	+	1.1
Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием	+	+	+	+	+	+	+	+	+	+	2.1
Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы	+	+	+	+	+	+	+	+	+	+	4.3
Обеспечение резервирования сетевого оборудования по схеме N + 1	±	±	±	±	±	±	±	±	+	+	6.5

Продолжение таблицы 2

1	2	3	4	5	6	7	8	9	10	11	12
Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	±	±	±	±	+	±	±	±	±	+	6.6
Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	+	+	+	+	+	+	+	+	+	+	7.1
Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы)	+	+	+	+	+	+	+	+	+	+	7.4
Определение состава и содержания информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+	7.5
Обеспечение резервирования информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+	7.6
Обеспечение резервирования конфигурационных файлов сетевого оборудования	±	±	+	±	+	+	+	+	+	+	7.7
Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления	+	+	+	+	+	+	+	+	+	+	7.8
Определение перечня внешних подключений к информационной системе и порядка такого подключения	±	±	±	±	±	+	+	+	+	+	7.19

Примечание – Классы 5–14 соответствуют классам типовых информационных систем, приведенным в таблице 1; требования, отмеченные знаком «+», являются обязательными; требования, отмеченные знаком «±», являются рекомендуемыми; колонка «Подпункт [10]» содержит номер подпункта, соответствующего требованиям из перечня, указанного в таблице Д.1 (приложение Д).

Важно отметить следующее [11–13]:

– на выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, распространяется действие технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375;

– средства защиты информации выпускаются в обращение на рынке в установленном порядке при их соответствии техническому регламенту ТР 2013/027/BY, а также другим техническим регламентам, действие которых на них распространяется;

– средства защиты информации, соответствие которых требованиям технического регламента ТР 2013/027/BY не подтверждено, не маркируются знаком соответствия техническому регламенту и не допускаются к выпуску в обращение на рынке;

– реестры [12; 13] включают перечни продуктов информационных технологий, прошедших экспертизу и сертификацию соответственно.

Таким образом, на практике при выборе технических средств защиты информации, необходимых к реализации, целесообразно использовать перечень сертифицированных продуктов информационных технологий [13] с учетом:

– применяемых технологий, типовых классов, к которым относятся информационные системы, а также обязательных и рекомендуемых требований (см. практические занятия 1 и 2), определенных в техническом задании на создание систем защиты информации;

– соответствующих параметров информационных систем, которые показаны на рисунке 14.

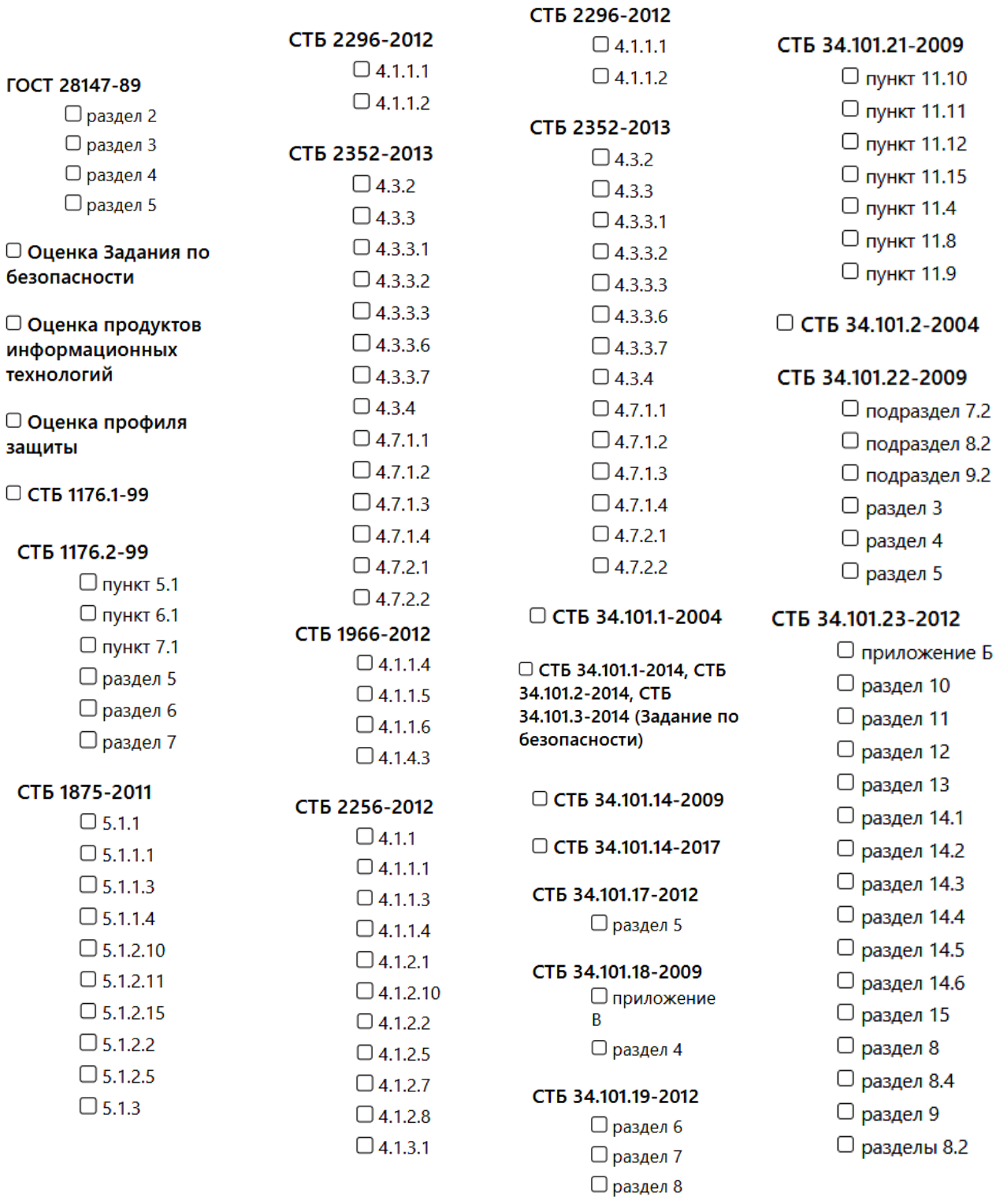


Рисунок 14 – Параметры, учитываемые при выборе технических средств защиты информации [13]

СТБ 34.101.26-2012 (подпункты)
- ☐ пункт 5.10.2
- ☐ пункт 5.8
- ☐ пункт 6.1
- ☐ пункт 6.2
- ☐ раздел 6

СТБ 34.101.27-2011
- ☐ класс 1
- ☐ класс 2
- ☐ подраздел 5.1
- ☐ подраздел 5.2
- ☐ подраздел 5.3
- ☐ подраздел 5.4
- ☐ подраздел 5.5
- ☐ подраздел 5.6
- ☐ подраздел 6.1
- ☐ подраздел 6.2
- ☐ подраздел 7.1
- ☐ подраздел 7.2
- ☐ подраздел 7.3
- ☐ подраздел 7.4
- ☐ пункт 5.6 класса 2
- ☐ раздел 6
- ☐ раздел 7

СТБ 34.101.27-2022
- ☐ пункт 5.10
- ☐ пункт 5.11
- ☐ пункт 5.12
- ☐ пункт 6.3
- ☐ уровень 1
- ☐ уровень 2
- ☐ уровень 3
- ☐ уровень 4

СТБ 34.101.28-2011
- ☐ 4.2
- ☐ 4.3.1
- ☐ 4.3.10
- ☐ 4.3.2
- ☐ 4.3.5
- ☐ 4.3.6
- ☐ 4.3.7
- ☐ 4.3.8
- ☐ 4.3.9

СТБ 34.101.29-2011
- ☐ 4.2

☐ **СТБ 34.101.29-2012**

СТБ 34.101.31-2011
- ☐ подраздел 6.1
- ☐ подраздел 6.2
- ☐ подраздел 6.3
- ☐ подраздел 6.4
- ☐ подраздел 6.5
- ☐ подраздел 6.6
- ☐ подраздел 6.7
- ☐ подраздел 6.8
- ☐ подраздел 6.9
- ☐ подраздел 7.1
- ☐ подраздел 7.2
- ☐ раздел 6
- ☐ раздел 7

СТБ 34.101.31-2020
- ☐ приложение В
- ☐ пункт 7.10
- ☐ пункт 7.2
- ☐ пункт 7.3
- ☐ пункт 7.4
- ☐ пункт 7.5
- ☐ пункт 7.6 схема 1
- ☐ пункт 7.6 схема 2
- ☐ пункт 7.8
- ☐ пункт 7.9
- ☐ пункт 8.1
- ☐ пункт 8.2

☐ **СТБ 34.101.3-2004**

СТБ 34.101.37-2017
- ☐ 7.2
- ☐ 7.3

СТБ 34.101.45-2013
- ☐ подраздел 5
- ☐ подраздел 6.1.1
- ☐ подраздел 6.1.2
- ☐ подраздел 6.1.4
- ☐ подраздел 6.2
- ☐ подраздел 6.2.1
- ☐ подраздел 6.2.2
- ☐ подраздел 6.3
- ☐ подраздел 7
- ☐ подраздел 7.1
- ☐ подраздел 7.2
- ☐ приложение А
- ☐ приложение Б
- ☐ приложение В
- ☐ приложение Г
- ☐ приложение Д
- ☐ приложение Е
- ☐ приложение Ж
- ☐ пункт 6.2
- ☐ пункт 6.3
- ☐ пункт 7.2
- ☐ таблица Б1
- ☐ таблица Б2
- ☐ таблица Б3

СТБ 34.101.47-2012
- ☐ пункт 6.1
- ☐ пункт 6.2
- ☐ пункт 6.3

СТБ 34.101.47-2017
- ☐ пункт 6.1
- ☐ пункт 6.2
- ☐ пункт 6.3
- ☐ раздел 6

☐ **СТБ 34.101.48-2012**

СТБ 34.101.49-2012
- ☐ раздел 10
- ☐ раздел 11
- ☐ раздел 6
- ☐ раздел 8
- ☐ раздел 9

СТБ 34.101.50-2012
- ☐ приложение Б
- ☐ приложение В
- ☐ приложение Г
- ☐ приложение Д

СТБ 34.101.50-2019
- ☐ приложение В
- ☐ приложение Е

☐ **СТБ 34.101.51-2011**

СТБ 34.101.60-2014
- ☐ приложение А
- ☐ раздел 7
- ☐ таблица А1

☐ **СТБ 34.101.65-2014**

СТБ 34.101.65-2014 (подпункты)
- ☐ подпункт В2.5.1
- ☐ подпункт В2.5.2
- ☐ подпункт В2.5.3
- ☐ подпункт В2.5.4
- ☐ приложение В
- ☐ раздел 10
- ☐ раздел 6
- ☐ раздел 7
- ☐ раздел 8
- ☐ раздел 9

СТБ 34.101.66-2014
- ☐ подраздел 7.4
- ☐ подраздел 7.5
- ☐ подраздел 7.6
- ☐ приложение А
- ☐ пункт 6.1
- ☐ пункт 7.4
- ☐ пункт 7.5
- ☐ пункт 7.6

Рисунок 14, лист 2

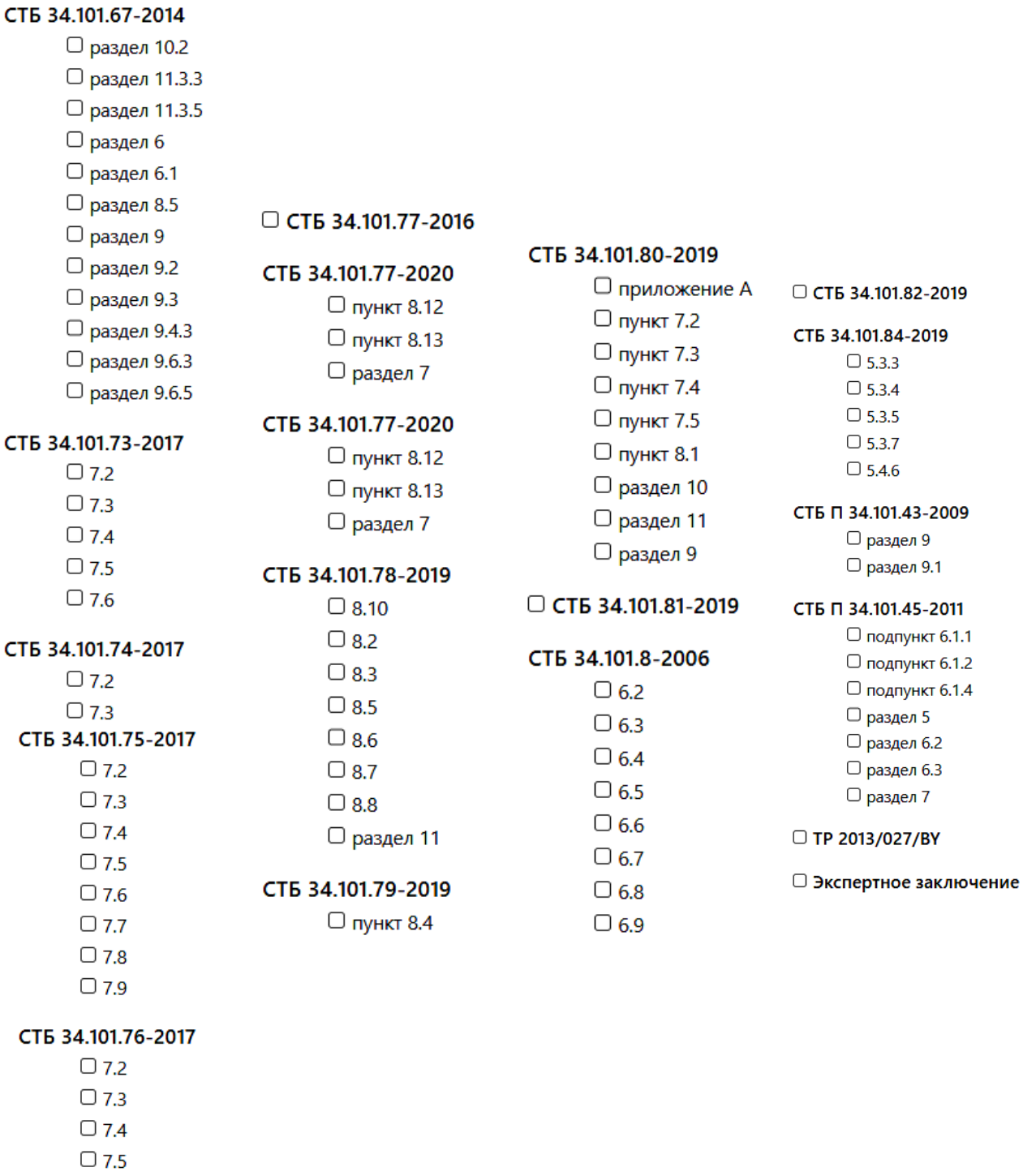


Рисунок 14, лист 3

3.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCriptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCriptoLab.exe» активируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «Выбор средств и мер защиты информации для ТИС» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Главу:» – «ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ»;

2) пункт «2 Раздел:» – «ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ»;

3) пункт «3 Тему:» – «ВЫБОР СРЕДСТВ И МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ТИС».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы, показанное на рисунке 15.

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы.

Рисунок 15 – Общий план выполнения задания по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 15) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 16, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 17.

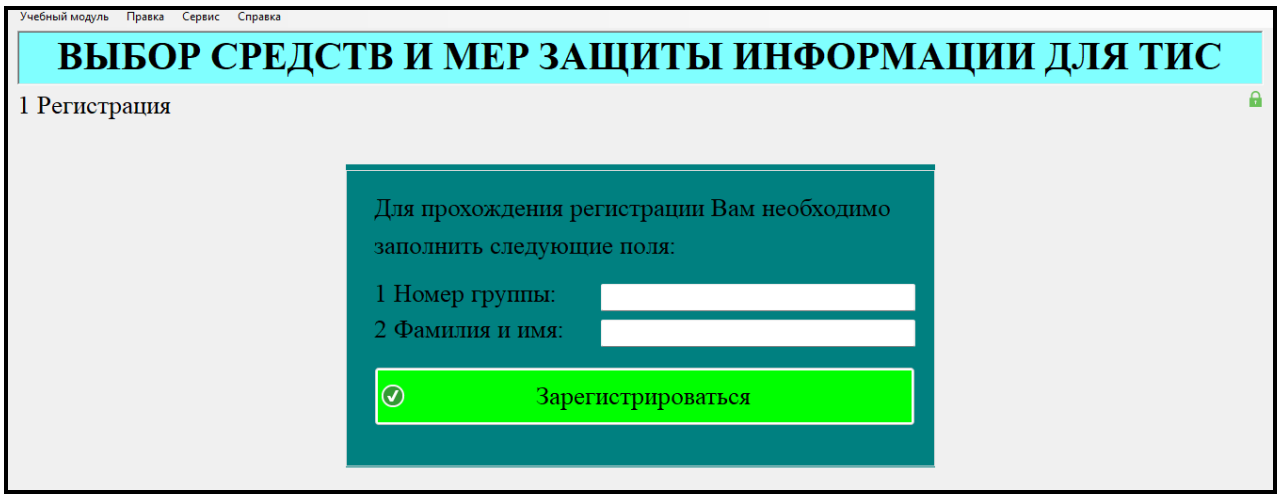


Рисунок 16 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

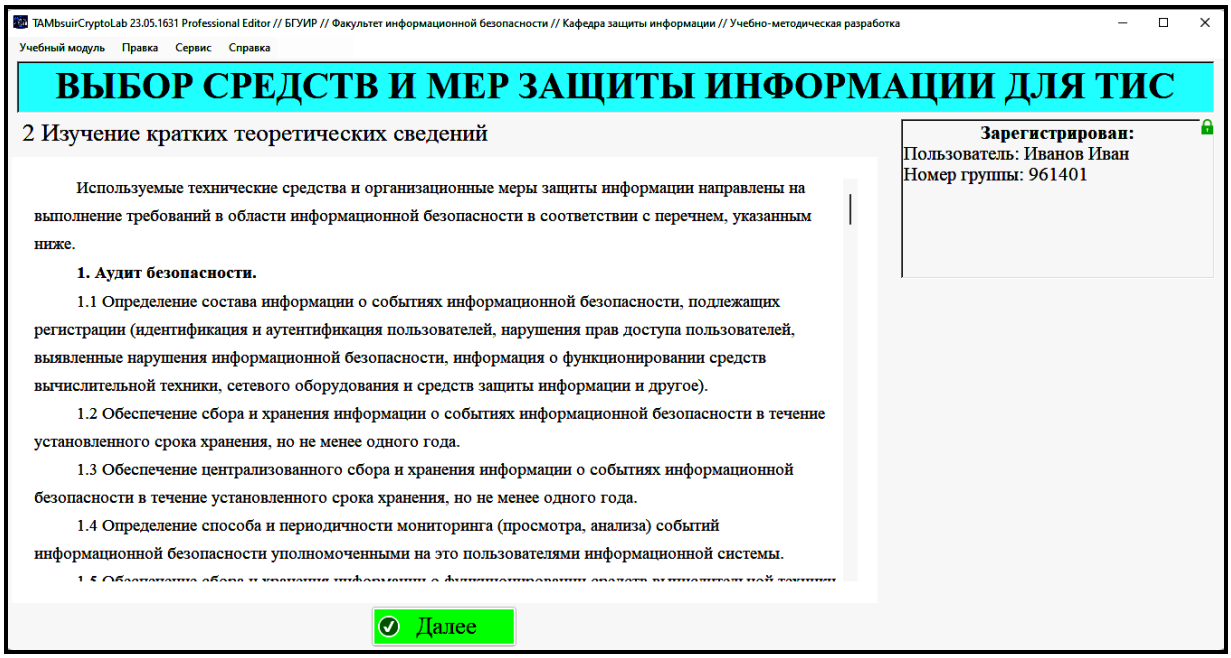


Рисунок 17 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 17) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 18, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

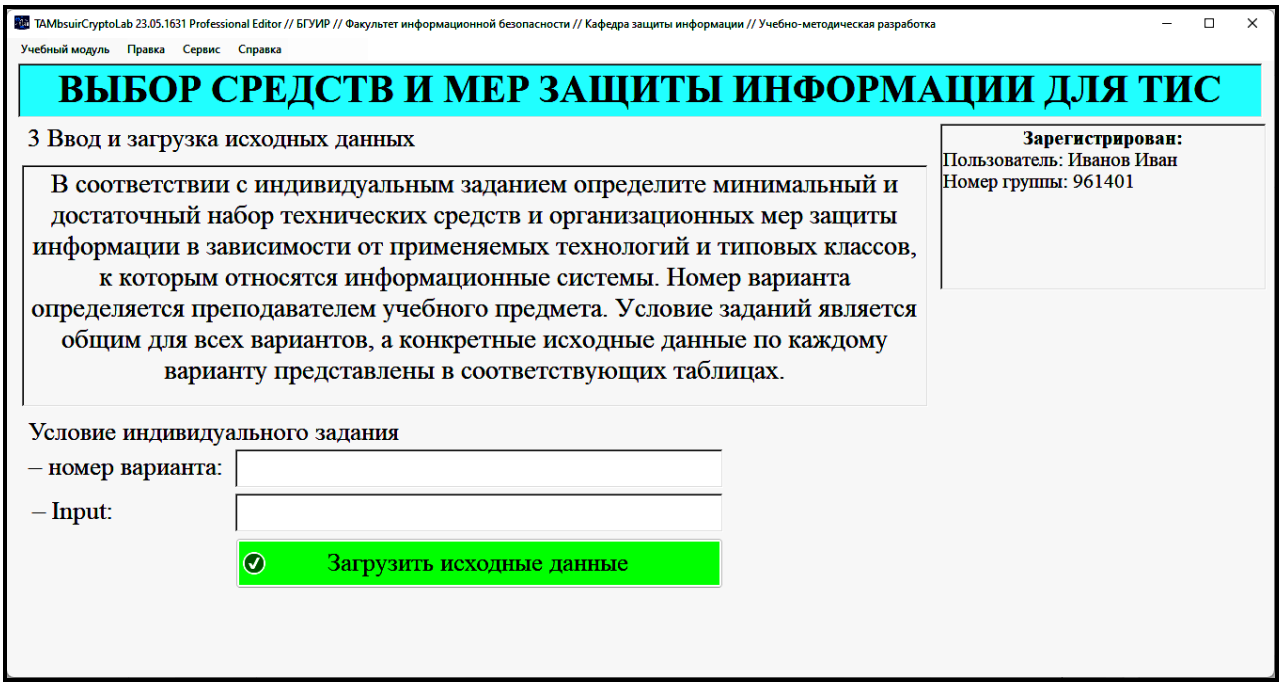


Рисунок 18 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению методики определения минимального и достаточного набора технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

В результате на экране появится окно, соответствующее этапу 4 общего плана задания (рисунок 19) по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации для типовых информационных систем.

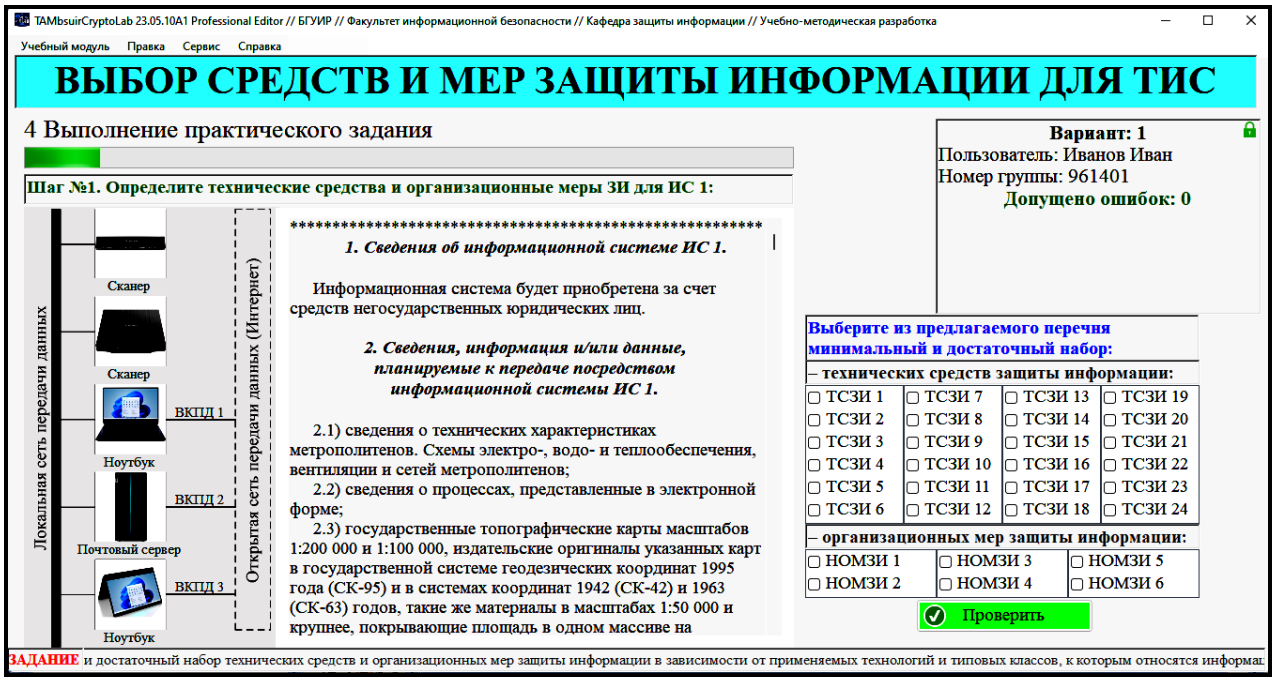


Рисунок 19 – Внешний вид окна по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

5 Выполните предлагаемые задания по определению минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы.

Номер варианта задания определяется преподавателем дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 19, и заключается в пошаговом определении минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде бегущей строки.

Суть выполнения каждого шага задания заключается в изучении предлагаемого варианта построения информационной системы, оценке ее типового класса (типовых классов), а также обязательных и рекомендуемых требований, предъявляемых к системе защиты информации, и на основании этого определении минимальных и достаточных наборов технических средств и организационных мер защиты информации путем выбора соответствующих пунктов (см. нижнюю правую область окна с подзаголовками «Выберите из предлагаемого перечня минимальный и достаточный набор технических средств защиты информации:» и «Выберите из предлагаемого перечня минимальный и достаточный набор организационных мер защиты информации:»).

Чтобы выбрать пункт, необходимо нажать на него, после чего пункт будет отмечен галочкой; при повторном нажатии выбор пункта отменяется, и галочка снимается. Галочки необходимо установить рядом с теми пунктами, которые соответствуют предлагаемому варианту информационной системы.

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если один или несколько пунктов выбран (выбраны) неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от

применяемых технологий и типовых классов, к которым относятся информационные системы (см. рисунок 19).

Задание по определению минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы, считается выполненным, если все шаги завершены успешно.

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю дисциплины.

Задание считается выполненным, если пункты 1–6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 20, *а*.

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 20, *б*. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш Ctrl + J, в появившемся окне (рисунок Г.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2–7 практического задания.

а

б

а – задание выполнено; *б* – задание не выполнено

Рисунок 20 – Заключительные результаты выполнения задания по изучению методики определения минимальных и достаточных наборов технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы

3.3 Содержание отчета

1 Цель практического занятия.

2 Краткие теоретические сведения о методике определения минимального и достаточного набора технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

3.4 Контрольные вопросы

1 Каким образом при определении минимального и достаточного набора технических средств и организационных мер защиты информации учитываются типовые классы, к которым относятся информационные системы?

2 Какие обязательные организационные меры защиты информации свойственны для информационных систем любого типового класса?

3 Какие обязательные организационные меры защиты информации различаются в зависимости типовых классов, к которым относятся информационные системы?

4 В чем заключается сущность методики определения минимального и достаточного набора технических средств и организационных мер защиты информации в зависимости от применяемых технологий и типовых классов, к которым относятся информационные системы?

5 К какому наибольшему количеству типовых классов одновременно может относиться одна и та же информационная система, для которой необходимо определить минимальный и достаточный набор технических средств и организационных мер защиты информации?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 4.
ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Цель: изучение требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем.

4.1 Краткие теоретические сведения

При организации взаимодействия типовой информационной системы с иными типовыми информационными системами важно определить порядок такого взаимодействия. Эта работа проводится на этапе проектирования системы защиты информации и отражается в техническом задании на создание системы защиты информации в виде соответствующих сведений согласно данным из таблицы Е.1 (приложение Е).

На этапе создания системы защиты информации осуществляются:

– внедрение средств технической и криптографической защиты информации, проверка их работоспособности и совместимости с другими объектами информационной системы;

– разработка (корректировка) документации на систему защиты информации по перечню, определенному в техническом задании;

– реализация организационных мер по защите информации.

В ходе внедрения средств технической и криптографической защиты информации осуществляются:

– их монтаж и наладка в соответствии с документацией на систему защиты информации, рекомендациями изготовителя, требованиями по совместимости средств криптографической защиты информации и ограничениями, указанными в сертификате соответствия;

– смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию, либо блокировка учетных записей, не предусматривающих смену указанных реквизитов;

– проверка корректности выполнения такими средствами требований безопасности в реальных условиях эксплуатации и во взаимодействии с другими объектами информационной системы.

Документация на систему защиты информации должна содержать описание способов разграничения доступа пользователей к объектам информационной системы, а также порядок:

– резервирования и уничтожения информации;

– защиты от вредоносного программного обеспечения;

– использования съемных носителей информации и электронной почты;

– обновления средств защиты информации;

– осуществления контроля (мониторинга) за функционированием информационной системы и системы защиты информации;

– реагирования на события информационной безопасности и ликвидации их последствий;

– управления криптографическими ключами, в том числе требования по их генерации, распределению, хранению, доступу к ним и их уничтожению.

В случае документирования создания информационных систем в соответствии с техническими нормативными правовыми актами, регламентирующими порядок создания автоматизированных систем, сведения, указанные в пункте 17 Приказа Оперативно-аналитического центра при Президенте Республики Беларусь «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [10], могут быть предусмотрены в документах на автоматизированную информационную систему.

Реализация организационных мер по защите информации осуществляется в целях выполнения требований, изложенных в документации на систему

защиты информации собственника (владельца) информационной системы, которые доводятся до сведения пользователей информационной системы под роспись.

Организационные меры по криптографической защите информации должны включать в себя меры по обеспечению особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к средствам криптографической защиты информации и криптографическим ключам (носителям), а также по разграничению доступа к ним по кругу лиц (см. практическое занятие 3).

При получении собственником (владельцем) информационной системы от физического лица его персональных данных, предоставленных этим физическим лицом без использования средств криптографической защиты информации, предоставление в последующем этих данных тем же собственником (владельцем) информационной системы названному физическому лицу может осуществляться без использования средств криптографической защиты информации [10].

В процессе эксплуатации информационной системы с применением аттестованной в установленном порядке системы защиты информации осуществляются:

– контроль за соблюдением требований, установленных в нормативных правовых актах, документации на систему защиты информации собственника (владельца) информационной системы;

– контроль за порядком использования объектов информационной системы;

– мониторинг функционирования системы защиты информации;

– выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования информационной системы;

– резервное копирование информации, содержащейся в информационной системе;

– обучение (повышение квалификации) пользователей информационной системы.

В соответствии с документацией на систему защиты информации собственники (владельцы) информационных систем выявляют и фиксируют нарушения требований по защите информации, принимают меры по своевременному устранению таких нарушений.

В случае компрометации криптографических ключей средств криптографической защиты информации собственники (владельцы) информационных систем обязаны незамедлительно прекратить использование данных средств для обработки информации.

В случае невозможности устранения выявленных нарушений в течение пяти рабочих дней с момента их выявления собственники (владельцы) информационных систем обязаны:

– прекратить обработку информации, распространение и (или) предоставление которой ограничено, о чем письменно информировать ОАЦ;

– осуществить доработку системы защиты информации и провести оценку на предмет необходимости ее повторной аттестации.

Наладочные работы и сервисное обслуживание объектов информационной системы проводятся с участием подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации, если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами.

Модернизация действующих систем защиты информации осуществляется в порядке, установленном Приказом Оперативно-аналитического центра при Президенте Республики Беларусь «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [10] для проектирования и создания таких систем.

В случае прекращения эксплуатации информационной системы собственник (владелец) информационной системы в соответствии с документацией на систему защиты информации принимает меры:

– по защите информации, которая обрабатывалась в информационной системе;

– резервному копированию информации и криптографических ключей (при необходимости), обеспечению их конфиденциальности и целостности;

– уничтожению (удалению) данных и криптографических ключей с машинных носителей информации и (или) уничтожению таких носителей информации.

4.2 Практическое задание

1 Включите персональный компьютер и запустите файл «TAMbsuirCriptoLab.exe» на выполнение.

После запуска файла «TAMbsuirCriptoLab.exe» активируется программное обеспечение, и появится окно выбора задания для выполнения (см. рисунок 1).

2 Выберите задание «Требования к организации взаимодействия ТИС» и ознакомьтесь с общим планом его выполнения.

Для выбора задания необходимо в окне, показанном на рисунке 1, последовательно указать следующее:

1) пункт «1 Главу:» – «ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ»;

2) пункт «2 Раздел:» – «ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ»;

3) пункт «3 Тему:» – «ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ТИС».

Затем нажмите кнопку «Перейти к заданию». В результате появится окно, содержащее общий план выполнения задания по изучению требований к

организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем, показанное на рисунке 21.

Рисунок 21 – Общий план выполнения задания по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем

3 Зарегистрируйтесь и ознакомьтесь с краткими теоретическими сведениями по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем.

Для того чтобы зарегистрироваться, необходимо в окне с общим планом выполнения задания (см. рисунок 21) нажать кнопку «Приступить к выполнению задания» и в появившемся окне регистрации, приведенном на рисунке 22, указать номер своей группы в поле «1 Номер группы:», ввести свою фамилию и имя в поле «2 Фамилия и имя:» и нажать кнопку «Зарегистрироваться».

После этого появится окно с краткими теоретическими сведениями, показанное на рисунке 23.

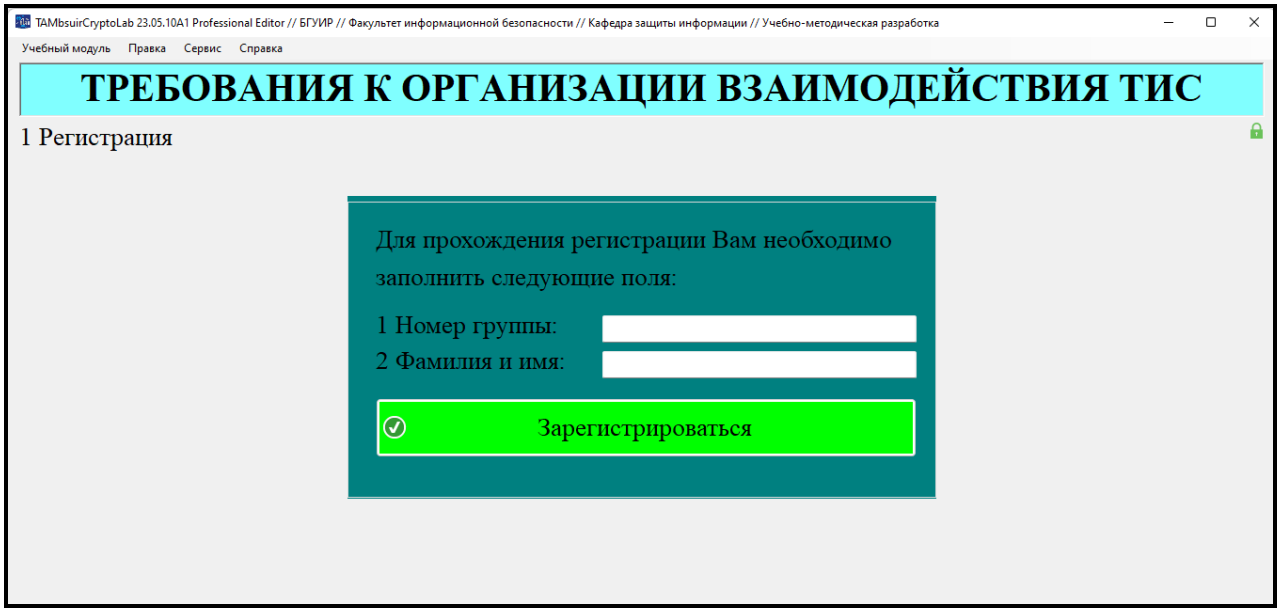
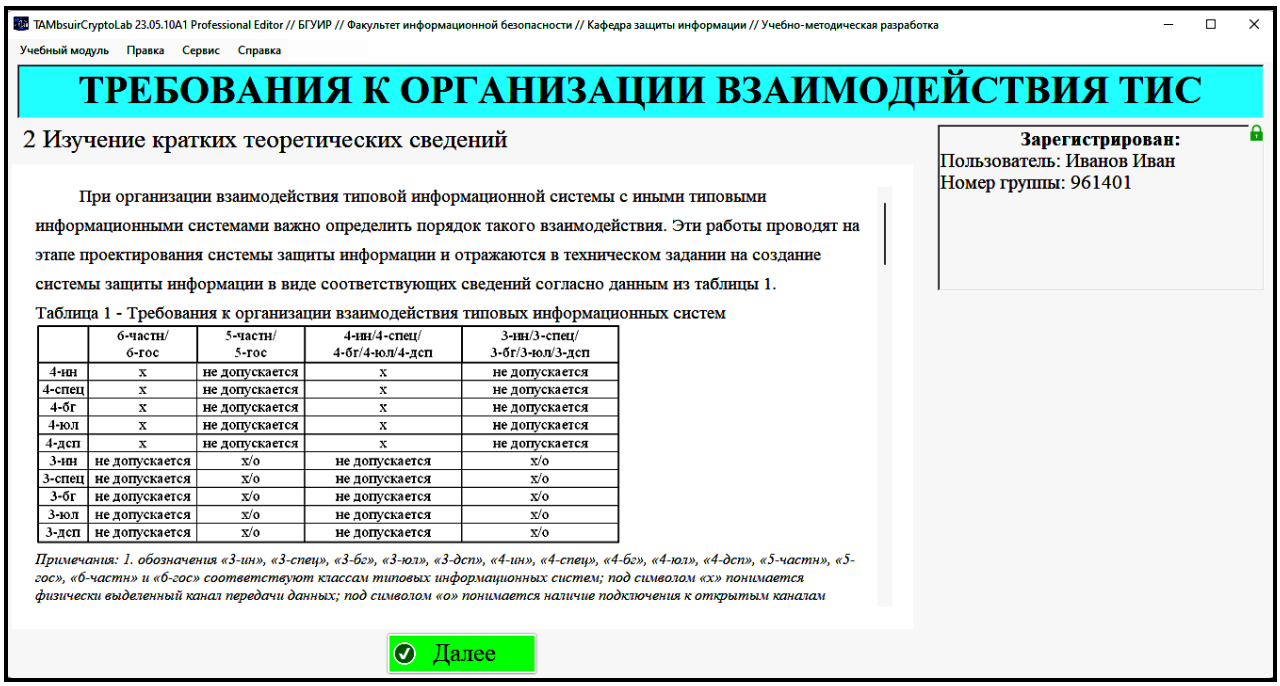


Рисунок 22 – Внешний вид окна регистрации, соответствующего этапу 1 общего плана задания по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем



При организации взаимодействия типовой информационной системы с иными типовыми информационными системами важно определить порядок такого взаимодействия. Эти работы проводят на этапе проектирования системы защиты информации и отражаются в техническом задании на создание системы защиты информации в виде соответствующих сведений согласно данным из таблицы 1.

Таблица 1 - Требования к организации взаимодействия типовых информационных систем

	6-частн/ 6-гос	5-части/ 5-гос	4-ин/4-спец/ 4-бг/4-юл/4-дсп	3-ин/3-спец/ 3-бг/3-юл/3-дсп
4-ин	х	не допускается	х	не допускается
4-спец	х	не допускается	х	не допускается
4-бг	х	не допускается	х	не допускается
4-юл	х	не допускается	х	не допускается
4-дсп	х	не допускается	х	не допускается
3-ин	не допускается	х/о	не допускается	х/о
3-спец	не допускается	х/о	не допускается	х/о
3-бг	не допускается	х/о	не допускается	х/о
3-юл	не допускается	х/о	не допускается	х/о
3-дсп	не допускается	х/о	не допускается	х/о

Примечания: 1. обозначения «3-ин», «3-спец», «3-бг», «3-юл», «3-дсп», «4-ин», «4-спец», «4-бг», «4-юл», «4-дсп», «5-частн», «5-гос», «6-частн» и «6-гос» соответствуют классам типовых информационных систем; под символом «х» понимается физически выделенный канал передачи данных; под символом «о» понимается наличие подключения к открытым каналам

Рисунок 23 – Внешний вид окна с краткими теоретическими сведениями, соответствующего этапу 2 общего плана задания по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем

4 Загрузите исходные данные в соответствии с индивидуальным вариантом, который определяется преподавателем дисциплины.

Для загрузки исходных данных необходимо в окне с краткими теоретическими сведениями (см. рисунок 23) нажать кнопку «Далее» и в появившемся окне ввода и загрузки исходных данных, приведенном на рисунке 24, ввести исходные данные и нажать кнопку «Загрузить исходные данные».

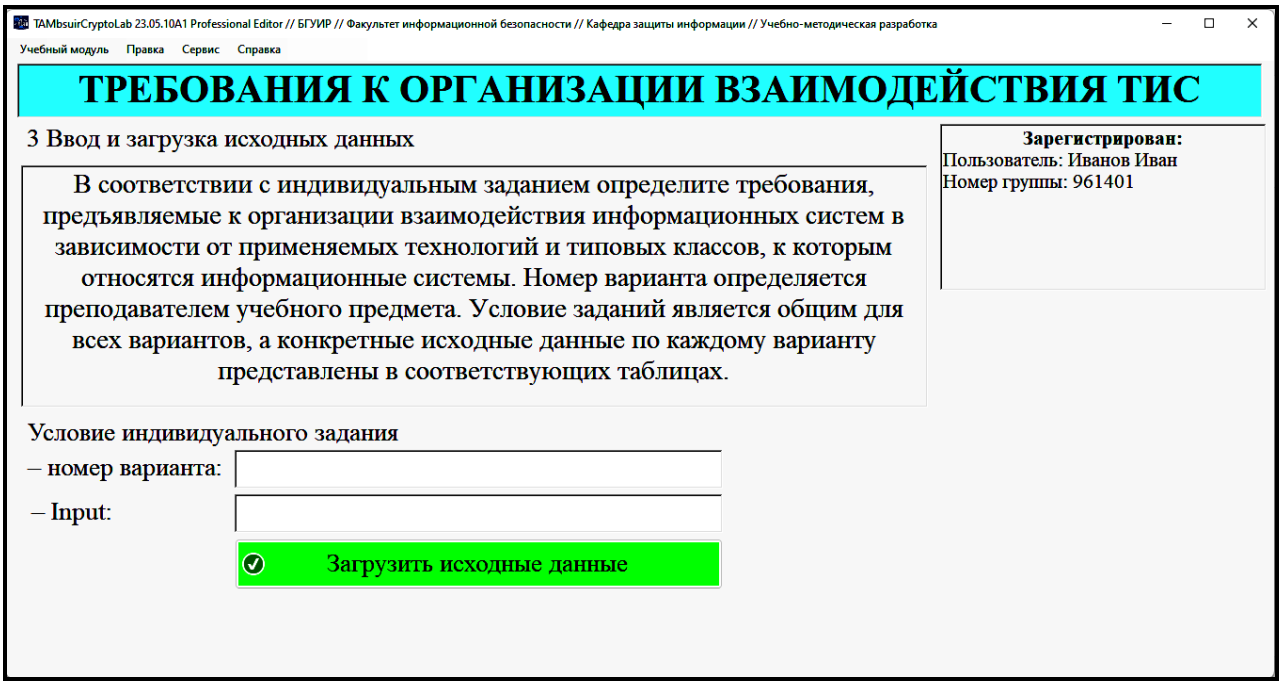


Рисунок 24 – Внешний вид окна ввода и загрузки исходных данных, соответствующего этапу 3 общего плана задания по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем

В результате на экране появится окно, соответствующее этапу 4 общего плана задания (рисунок 25) по определению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем.

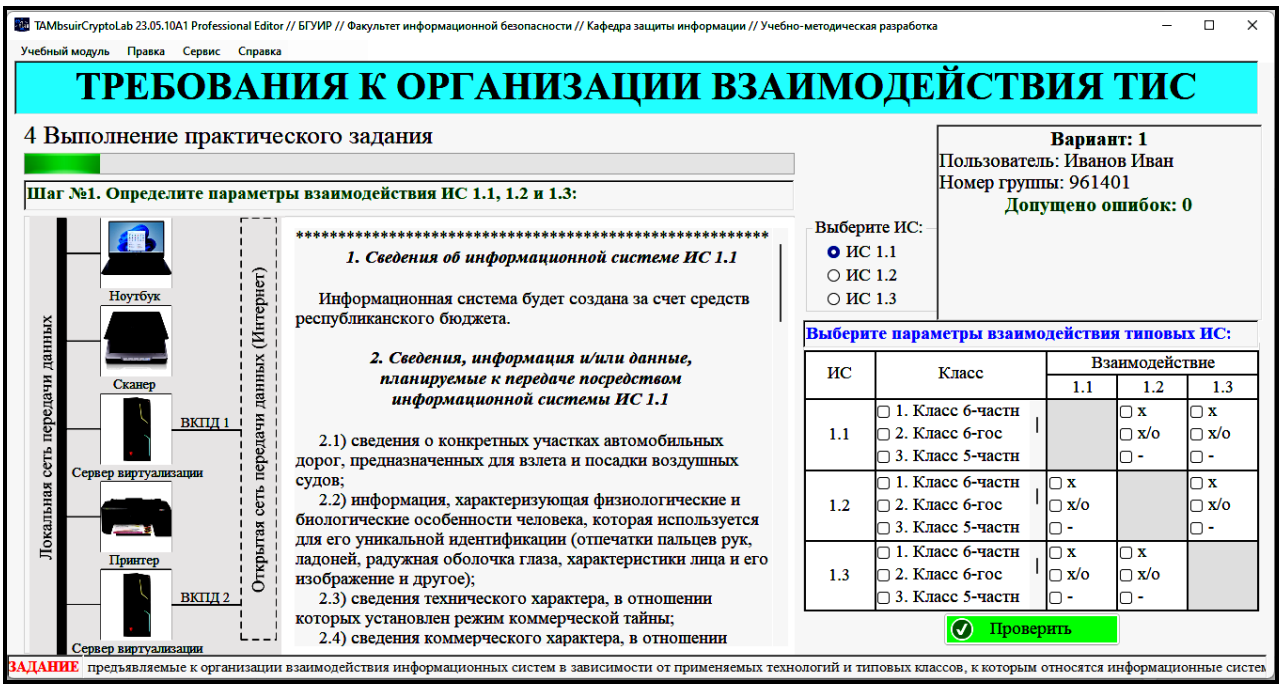


Рисунок 25 – Внешний вид окна по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем

5 Выполните предлагаемые задания по определению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем.

Номер варианта задания определяется преподавателем дисциплины. Условие заданий является общим для всех вариантов, а конкретные исходные данные по каждому варианту представлены в соответствующих таблицах.

Задание выполняется в окне, представленном на рисунке 25, и заключается в пошаговом определении требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем. Для удобства работы с программой текст задания дублируется в нижней части этого окна в виде бегущей строки.

Суть выполнения каждого шага задания заключается в изучении предлагаемых вариантов построения информационных систем, оценке типового

класса (типовых классов) каждой из них и на основании этого определения требований к организации взаимодействия информационных систем путем выбора соответствующих пунктов (см. рисунок 25, нижнюю правую область окна с подзаголовком «Выберите параметры взаимодействия типовых ИС:»):

– «х»: взаимодействие посредством физически выделенных каналов передачи данных;

– «х/о»: взаимодействие либо посредством физически выделенных каналов передачи данных, либо с помощью открытых каналов передачи данных (в том числе глобальной компьютерной сети Интернет);

– «–»: взаимодействие не допускается.

Чтобы выбрать пункт, необходимо нажать на него, после чего он будет отмечен галочкой; при повторном нажатии выбор пункта отменяется, и галочка снимается. Галочки необходимо установить рядом с теми пунктами, которые соответствуют предлагаемому варианту информационных систем.

Чтобы проверить правильность выполнения каждого шага задания, необходимо нажать кнопку «Проверить».

Если один или несколько пунктов выбраны неверно, на экран выводится сообщение об ошибке. В этом случае необходимо закрыть окно с сообщением об ошибке и повторно выполнить задание в окне по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем (см. рисунок 25).

Задание по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем считается выполненным, если все шаги завершены успешно.

6 Выполните тестовое задание, соответствующее этапу 5 общего плана задания.

Окно с тестовыми заданиями отображается автоматически после завершения этапа 4 общего плана задания. Тест содержит 10 вопросов. Необходимо ответить на все вопросы. Правильных ответов может быть несколько.

Тестовые задания считаются выполненными, если все предлагаемые задания завершены успешно.

7 Продемонстрируйте результаты выполнения задания преподавателю дисциплины.

Задание считается выполненным, если пункты 1–6 практического задания завершены успешно. При этом на экран выводится окно, показанное на рисунке 26, *а*.

Задание считается невыполненным, если на экран выводится окно, показанное на рисунке 26, *б*. В этом случае необходимо отменить загруженный учебный модуль, нажав комбинацию клавиш Ctrl + J, в появившемся окне (рисунок Г.3) подтвердить отмену, выбрав «Да», и заново выполнить пункты 2–7 практического задания.

4.3 Содержание отчета

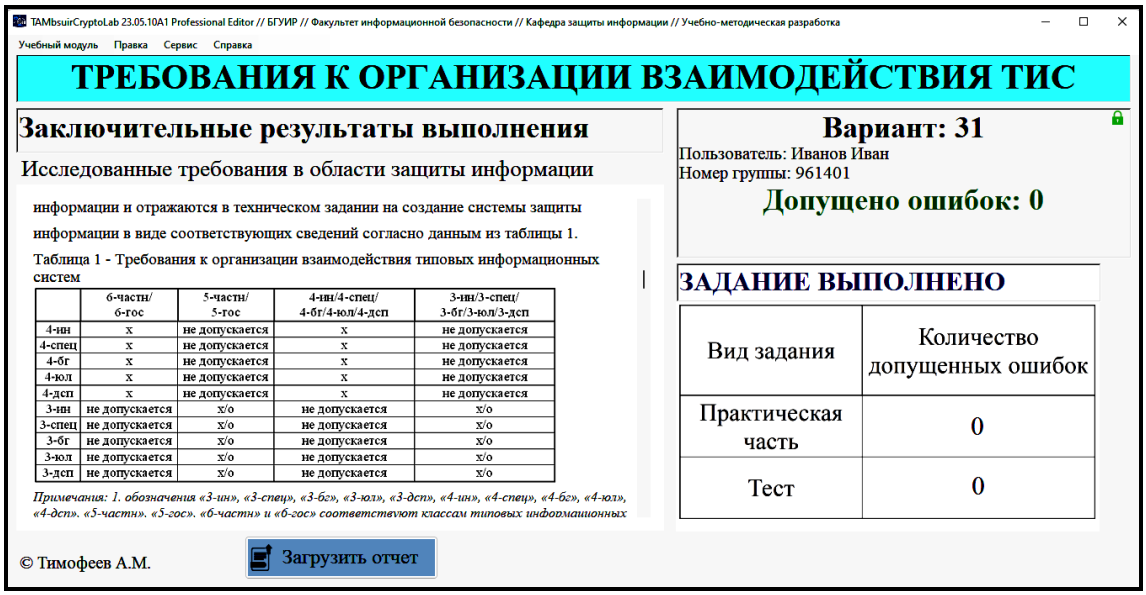
1 Цель практического занятия.

2 Краткие теоретические сведения о требованиях, предъявляемых к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем.

3 Выводы по результатам выполнения практических заданий.

4 Ответы на контрольные вопросы.

а



б

а – задание выполнено; *б* – задание не выполнено

Рисунок 26 – Заключительные результаты выполнения задания по изучению требований к организации взаимодействия информационных систем в зависимости от применяемых технологий и классов типовых информационных систем

4.4 Контрольные вопросы

1 В соответствии с каким основным нормативно-правовым документом в Республике Беларусь проводятся работы по организации взаимодействия типовых информационных систем?

2 Какие каналы передачи данных допускается использовать при организации взаимодействия типовых информационных систем и что определяет тип выбираемого канала?

3 В каких случаях организация взаимодействия типовых информационных систем не допускается?

4 К какому наибольшему количеству типовых классов одновременно может относиться одна и та же информационная система, для которой необходимо определить порядок организации взаимодействия с другой типовой информационной системой?

5 Влияют ли структуры информационных систем, их физические и логические границы, а также содержание информационных потоков (внутренних и внешних) на порядок организации взаимодействия информационных систем? Если да, то каким образом?

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ

База данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях.

Банк данных – это организационно-техническая система, включающая одну или несколько баз данных и систему управления ими.

Биометрические персональные данные – это информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое).

Владелец информационных систем – это субъект информационных отношений, реализующий права владения, пользования и распоряжения информационными системами в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь.

Владелец коммерческой тайны – это юридическое или физическое лицо, в том числе индивидуальный предприниматель, а также государственный орган, иностранная организация, не являющаяся юридическим лицом, правомерно обладающие сведениями, в отношении которых установлен режим коммерческой тайны, за исключением случаев, когда эти сведения составляют коммерческую тайну других лиц.

Генетические персональные данные – это информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца.

Государственная информационная система – это информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Государственный информационный ресурс – это информационный ресурс, формируемый или приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Документированная информация – это информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.

Доступ к информации – это возможность получения информации и пользования ею.

Доступ к информационной системе – это возможность использования информационной системы.

Доступ к коммерческой тайне – это возможность ознакомления с согласия владельца коммерческой тайны или на ином законном основании определенного круга лиц со сведениями, составляющими коммерческую тайну.

Защита информации – это комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации.

Информатизация – это организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений.

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная сеть – это совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи.

Информационная система – это совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационная технология – это совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Информационная услуга – это деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также защиты информации.

Информационные отношения – это отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Информационный посредник – это субъект информационных отношений, предоставляющий информационные услуги обладателям и (или) пользователям информации.

Информационный ресурс – это организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Коммерческая тайна – это сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), в отношении которых установлен режим коммерческой тайны.

Комплекс программно-технических средств – это совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий.

Контрагент – это сторона гражданско-правового договора (за исключением лиц, состоящих в трудовых отношениях с владельцем коммерческой тайны), которой владелец коммерческой тайны предоставляет доступ к сведениям, составляющим коммерческую тайну.

Конфиденциальность информации – это требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь.

Носитель коммерческой тайны – это документ или иной материальный объект, на котором сведения, составляющие коммерческую тайну, содержатся в любой объективной форме, в том числе в виде символов, образов, сигналов, позволяющих эти сведения распознать и идентифицировать.

Обладатель информации – это субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору.

Обработка персональных данных – это любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

Общедоступные персональные данные – это персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов.

Обязательство о неразглашении коммерческой тайны – это гражданско-правовой договор, заключаемый владельцем коммерческой тайны или лицом, получившим к ней доступ, с лицом, состоящим в трудовых отношениях с владельцем коммерческой тайны или лицом, получившим к ней доступ, и определяющий обязательства сторон, связанные с соблюдением конфиденциальности сведений, составляющих коммерческую тайну.

Оператор информационной системы – это субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги.

Разглашение коммерческой тайны – это действия (бездействие), в результате которых сведения, составляющие коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без согласия владельца коммерческой тайны или иного законного основания.

Режим коммерческой тайны – это правовые, организационные, технические и иные меры, принимаемые в целях обеспечения конфиденциальности сведений, составляющих коммерческую тайну.

Персональные данные – это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Пользователь информации – это субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею.

Пользователь информационной системы – это субъект информационных отношений, получивший доступ к информационной системе и пользующийся ею.

Предоставление информации – это действия, направленные на ознакомление с информацией определенного круга лиц.

Предоставление персональных данных – это действия, направленные на ознакомление с персональными данными определенного лица или круга лиц.

Распространение информации – это действия, направленные на ознакомление с информацией неопределенного круга лиц.

Распространение персональных данных – это действия, направленные на ознакомление с персональными данными неопределенного круга лиц.

Собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – это субъект

информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями.

Соглашение о конфиденциальности – это гражданско-правовой договор, заключаемый владельцем коммерческой тайны с контрагентом, предметом которого являются обязательства сторон по обеспечению конфиденциальности сведений, составляющих коммерческую тайну.

Специальные персональные данные – это персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные.

Средства защиты информации – средства защиты государственных секретов, средства криптографической защиты информации, средства технической защиты информации.

Средства защиты государственных секретов – технические, программные, криптографические и другие средства, используемые для защиты государственных секретов, а также средства контроля эффективности защиты государственных секретов.

Средства криптографической защиты информации – программные, программно-аппаратные средства, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности.

Средства технической защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации от несанкционированного доступа и несанкционированных воздействий на нее,

блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности.

Субъект персональных данных – это физическое лицо, в отношении которого осуществляется обработка персональных данных.

Удаление персональных данных – это действия, в результате которых становится невозможным восстановить персональные данные в информационных ресурсах (системах), содержащих персональные данные, и (или) в результате которых уничтожаются материальные носители персональных данных.

Уполномоченное лицо – это государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах.

Физическое лицо, которое может быть идентифицировано, – это физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

ПРИЛОЖЕНИЕ А

ПЕРЕЧЕНЬ СВЕДЕНИЙ, ОТНОСЯЩИХСЯ К СЛУЖЕБНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ [8]

Мобилизационные вопросы

1 Договоры на выполнение организациями независимо от организационно-правовых форм и форм собственности мобилизационных заданий (заказов) на поставку товаров, а также выполнение работ, оказание услуг в военное время.

2 Сведения в области мобилизационной подготовки и мобилизации (по организациям).

Наука и техника, научно-техническая информация

3 Сведения о конкретных разработчиках (в том числе фамилии, фотографии) вооружения, военной и специальной техники, о наличии закрытых научных советов, лабораторий.

4 Сведения о структурных схемах автоматизированных систем управления, сводные данные о компьютерной технике, оргтехнике и управляющих комплексах (по оборонному сектору экономики).

5 Сведения об экспорте (импорте) результатов научно-технической деятельности (наукоемких технологий, объектов интеллектуальной собственности), а также материалов научно-исследовательских, опытно-конструкторских работ, которые могут быть использованы при создании продукции военного назначения, товаров и технологий двойного назначения, которые могут быть применены при создании вооружений и военной техники.

Оборона и государственная безопасность

6 Сведения об организационно-штатной структуре, штатной численности правоохранительных и иных государственных органов и организаций.

7 Сведения о методах подготовки и проведения террористических актов, угонов самолетов и других особо опасных преступлений, о создании вооруженных организованных групп.

8 Сведения о силах, средствах, методах, планах, состоянии и результатах деятельности подразделений радиоэлектронной разведки и средствах связи.

9 Сведения об органах пограничной службы, раскрывающие:

– содержание мероприятий, направленных на реализацию планов по проведению государственной пограничной политики;

– организацию охраны Государственной границы Республики Беларусь, пограничного контроля, открытое распространение которых может создать риски обеспечения пограничной безопасности;

– систему и средства защиты информации в информационных системах органов пограничной службы;

– систему разграничения доступа к защищаемым информационным ресурсам, к действующим паролям, закрытым ключам электронно-цифровой подписи;

– систему охраны воинской части, организацию караульной службы, военизированной и сторожевой охраны, пропускного (объектового) режима, оснащение техническими средствами охраны конкретного объекта органов пограничной службы;

– укомплектованность должностей офицеров и прапорщиков;

– содержание приказов по личному составу;

– сводные данные об элементах оперативной обстановки на границе.

10 Сведения в сфере деятельности внутренних войск Министерства внутренних дел по обеспечению служебно-боевых задач.

11 Сведения о подготовке и проведении командно-штабных, оперативно-тактических мероприятий.

12 Сведения, содержащие сводные оценку состояния и прогноз развития оперативной обстановки в регионе.

13 Сведения, составляющие Государственный реестр критически важных объектов информатизации.

14 Сведения, полученные в результате проведения внешнего и внутреннего контроля критически важных объектов информатизации.

15 Сведения о системе безопасности критически важного объекта информатизации.

16 Сведения об организации систем и средств защиты информации в информационных системах таможенных органов.

17 Информация об организации и обеспечении защиты государственных секретов, не раскрывающая содержание технических мер защиты государственных секретов.

18 Сведения о предоставлении участков лесного фонда для нужд обороны.

Вопросы гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций, заимствования материальных ценностей

19 Декларации промышленной безопасности опасных производственных объектов.

20 Информация о составе оперативных групп и боевых расчетов пунктов управления.

21 Детализированные сведения по наиболее важным узлам и центрам управления опасных производств и объектов, эксплуатирующих в производстве аварийно и химически опасные вещества.

22 Информация, касающаяся физической защиты объектов, представляющих повышенную техногенную и экологическую опасность,

условно уязвимых в диверсионном отношении, в том числе в которых осуществляются хранение и (или) эксплуатация радионуклидных источников первой, второй и третьей категории по степени радиационной опасности.

23 Инструкции по операциям с материальными ценностями государственного материального резерва и о порядке их финансирования.

Военно-техническое сотрудничество

24 Сведения о содержании, подготовке, заключении и выполнении договоров, соглашений в сфере военно-технического сотрудничества с уполномоченными организациями иностранных государств до их государственной регистрации, если разглашение таких сведений повлечет негативные последствия для Республики Беларусь.

25 Сведения об экспорте (импорте), объемах выпуска и поставках (в стоимостном и натуральном выражении) продукции военного назначения, товаров и технологий двойного назначения, которые могут быть применены при создании вооружений и военной техники, а также о наличии и (или) наращивании мощностей по их выпуску, за исключением сведений, предоставляемых в рамках международных обязательств Республики Беларусь.

26 Обобщенные сведения о зарубежных командировках сотрудников республиканских органов государственного управления и (или) иных организаций по вопросам военно-технического сотрудничества.

27 Сведения о плановых мероприятиях по обеспечению защиты государственных секретов при осуществлении международного сотрудничества и посещении государственного органа, юридического лица представителями (делегациями, группами, отдельными гражданами) иностранных государств, международных организаций, межгосударственных образований.

Правоохранительная деятельность

28 Сведения, связанные с профессиональной деятельностью, разглашение которых может создать угрозу личной безопасности сотрудников правоохранительных органов и членов их семей, их имуществу.

29 Сведения о силах, средствах, формах и методах ведения предварительного расследования.

30 Сведения об органах прокуратуры в части обеспечения стоящих перед ними задач с учетом направлений деятельности.

31 Сведения о методах и способах производства оружия, взрывчатых веществ, средств инициирования пиротехнических составов.

32 Сведения о местонахождении баз, складов, количестве хранящихся на них взрывчатых и радиоактивных веществ, боевого огнестрельного оружия, сильнодействующих и ядовитых веществ, наркотических средств, психотропных веществ, их прекурсоров и аналогов.

33 Сведения о способах изготовления наркотических средств, психотропных веществ, их прекурсоров и аналогов.

34 Сведения о формах, методах, организации работы должностных лиц таможенных органов, используемых при этом силах и средствах, методике их применения при проведении специальных операций, таможенного контроля в отношении специфических товаров, при выявлении и пресечении контрабанды.

35 Сведения о новых формах и методах совершения контрабанды, административных таможенных правонарушений и мерах, принимаемых таможенными органами для выявления и пресечения этих правонарушений.

36 Сведения о формах и методах организации деятельности работников налоговых органов, органов Комитета государственного контроля, используемых при этом силах и средствах, методике их применения.

37 Сведения о новых формах и методах совершения правонарушений в области финансов, рынка ценных бумаг и банковской деятельности, предпринимательской деятельности, налогообложения, таможенных правонарушений и мерах, принимаемых налоговыми и другими контролирующими (надзорными) органами для выявления и пресечения этих правонарушений.

38 Сведения, содержащие результаты взаимодействия оперативных подразделений правоохранительных органов при выявлении (раскрытии) преступлений.

39 Сведения о дислокации постов и маршрутов патрулирования нарядами дорожно-патрульной службы Государственной автомобильной инспекции Министерства внутренних дел.

40 Сведения о работе органов и учреждений уголовно-исполнительной системы, лечебно-трудовых профилакториев Министерства внутренних дел при организации исполнения и отбывания наказаний, принудительной изоляции и медико-социальной реадаптации с обязательным привлечением к труду граждан, находящихся в лечебно-трудовых профилакториях, исполнения меры пресечения в виде заключения под стражу, актов амнистии и помилования, осуществления розыска лиц, уклоняющихся от отбывания наказания, принудительной изоляции и медико-социальной реадаптации с обязательным привлечением к труду (за исключением общедоступной информации).

41 Сведения об объемах отпуска хлебопродуктов спецпотребителям (исправительным учреждениям) в ассортименте.

Промышленность

42 Сведения по организациям о фондах заработной платы, количестве и обеспеченности специалистами, занятыми в производстве и разработке продукции военного назначения.

43 Сведения по организациям об объемах выпуска и поставках (в стоимостном или натуральном выражении) вооружения и военной техники, а также наличии или наращивании мощностей по их выпуску.

44 Сведения о работах в области технического нормирования и стандартизации, оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации,

обеспечения единства измерений в интересах обороны и военной безопасности, об испытаниях (надежность, живучесть, прочность), составе, рецептуре, технологии производства продукции военного и двойного назначения.

45 Направленные на создание (выпуск) продукции военного назначения планы развития, внедрения новой техники и новых технологических процессов, осуществления капитальных вложений, производства строительно-монтажных работ, ввода в действие основных фондов и сведения о выполнении этих планов (по организациям).

46 Сведения о местах хранения, системе охраны, наличии и количестве оружия и боеприпасов, взрывчатых веществ, применяемых для производственных нужд.

Энергетика

47 Сведения о количестве, точном местонахождении и емкости подземных хранилищ нефти, нефтепродуктов (по каждому отдельному хранилищу).

48 Сведения о количестве, точном местонахождении и емкости подземных хранилищ газа (по каждому отдельному хранилищу).

49 Привязка на генеральном плане местности схем отводов нефтепроводов и газопроводов, питающих электростанции.

50 Привязка на генеральном плане местности схем газоснабжения территорий, отнесенных к соответствующим категориям по гражданской обороне, газораспределительных станций и головных газорегуляторных пунктов.

51 Привязка на генеральном плане местности месторасположения газонаполнительных станций сжиженного газа, мощности их парков хранения.

52 Схемы энергетики регионов и объединенных энергосистем и их развития.

53 Схемы внешнего электроснабжения электрифицируемой железной дороги (существующие, проектируемые и планируемые на перспективу).

54 Генеральные планы, проекты и точное расположение (трассы) высоковольтных сетей напряжением 110000 В и выше.

55 Сведения о мощности и ее приросте, выработке электроэнергии действующих, строящихся и проектируемых электростанций и подстанций при организациях по выпуску средств связи, радиотехнической, электронной, авиационной продукции.

56 Сведения о мощности тяговых подстанций железной дороги (индивидуальная и суммарная).

57 Сведения о запасах и движении мазута на электростанциях, в государственном производственном объединении электроэнергетики «Белэнерго» и энергоснабжающих организациях, входящих в его состав.

Геология. Полезные ископаемые, их добыча и переработка

58 Технология получения из руды бериллия, лития, сведения о применяемом оборудовании и научно-исследовательские работы в этой области.

59 Сведения о промышленных мощностях по производству радиоактивных, трансурановых элементов (в том числе плутония), радиоактивных изотопов, их приросте, планы производства и сведения о их выполнении за любой период в натуральном или денежном выражении (по организациям).

Транспорт

60 Сведения о технических характеристиках метрополитенов. Схемы электро-, водо- и теплообеспечения, вентиляции и сетей метрополитенов.

61 Сведения о перевозках любыми видами транспорта валютных ценностей, драгоценных металлов и драгоценных камней, денежных знаков Республики Беларусь, взрывчатых, радиоактивных, сильнодействующих ядовитых и наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также о специальных железнодорожных перевозках и военных железнодорожных перевозках.

62 Сведения о дислокации воинских погрузочно-разгрузочных устройств, стационарных и подвижных военно-продовольственных пунктов, изоляционно-пропускных пунктов, дезинфекционных отрядов, законсервированных сооружений железнодорожной инфраструктуры и устройств, используемых в военное время.

63 Сведения, раскрывающие порядок действия членов экипажа и спецподразделений при захвате (попытке захвата, угона) воздушного судна.

64 Сведения о конкретных участках автомобильных дорог, предназначенных для взлета и посадки воздушных судов.

65 Сведения о порядке осуществления досмотра багажа пассажиров воздушного судна, в том числе вещей, находящихся при них.

Связь

66 Расписание движения автомобилей, перевозящих денежные средства, по почтовым маршрутам, информация о денежных средствах, перевозимых по почтовым маршрутам.

67 Утвержденные фельдъегерские маршруты и графики доставки корреспонденции подразделениями Государственной фельдъегерской службы Республики Беларусь при Министерстве связи и информатизации.

68 Сводные сведения о количественном и персональном составе сотрудников Государственной фельдъегерской службы Республики Беларусь при Министерстве связи и информатизации, наделенных статусом дипломатических курьеров Министерства иностранных дел.

69 Накопительные дела с документами о прохождении корреспонденции по каналам фельдъегерской связи и дипломатической почты по международным курьерским маршрутам.

70 Опознавательные сигналы и позывные радиостанций государственных органов, за исключением станций, открытых для международной службы общественной корреспонденции.

71 Схемы каналов трансляции телерадиопрограмм республиканского и иностранного вещания по каналам междугородной связи.

72 Сведения о закрытии радиостанций по решению Министерства обороны и Комитета государственной безопасности.

73 Сведения о подземных антеннах, телеграфировании, телефонировании через землю, сверхбыстродействующей, медленнодействующей и сверхдлинноволновой связи.

74 Сведения о мерах и технических средствах по защите от перехвата телеграфных сообщений и телефонных переговоров.

75 Схемы маршрутов по перевозке почты.

76 Информация о системах оборудования отделений связи различными видами сигнализации и технической укрепленности.

77 Информация, раскрывающая мероприятия по взаимодействию операторов электросвязи (за исключением оказывающих услуги по распространению программ телевизионного вещания и радиовещания) с органами, осуществляющими оперативно-розыскную деятельность:

– при построении сетей электросвязи с учетом требований по обеспечению внедрения и эксплуатации систем технических средств для обеспечения оперативно-розыскных мероприятий;

– оказании содействия в проведении оперативно-розыскных мероприятий и создании условий для их проведения на сетях электросвязи;

– обеспечении доступа к базам данных, автоматизированным системам операторов электросвязи, предоставлении информации о пользователях услуг электросвязи и об оказанных им услугах электросвязи, а также к иной информации, необходимой для выполнения задач, возложенных на органы, осуществляющие оперативно-розыскную деятельность.

Внешнеэкономическая деятельность. Финансы

78 Сведения, связанные с внешним государственным долгом Республики Беларусь и внешним долгом, гарантированным Республикой Беларусь:

– суммы просроченной задолженности по отдельным кредитам (займам), формирующим внешний государственный долг Республики Беларусь и внешний долг, гарантированный Республикой Беларусь;

– пролонгация платежей по погашению и обслуживанию кредитов (займов), формирующих внешний государственный долг Республики Беларусь и внешний долг, гарантированный Республикой Беларусь.

79 Сведения по торгово-экономическим вопросам военно-технического сотрудничества. Сводные сведения об эффективности, планах поставок, объемах экспорта или импорта продукции военного назначения, в том числе на условиях кредита, о поступлениях или платежах по этим операциям.

80 Сведения о размерах, состоянии и формировании Государственного фонда драгоценных металлов и драгоценных камней Республики Беларусь, а также об использовании его ценностей.

81 Дислокация, конструктивные решения, расположение инженерных коммуникаций, капитальных строений (зданий, сооружений) Государственного хранилища ценностей Министерства финансов.

82 Сведения о полном технологическом процессе разработки и производства бланков ценных бумаг и документов с определенной степенью защиты, документов с определенной степенью защиты, выпускаемых государством, и их полуфабрикатов, а также специальных материалов, иных методах и средствах их защиты от подделки.

83 Сведения о составе специальных материалов, применяемых для защиты от подделки бланков ценных бумаг и документов с определенной степенью защиты, документов с определенной степенью защиты, выпускаемых государством, и (или) химического реагента для определения их подлинности при экспертизе.

84 Сведения о значении кода специальных материалов для защиты от подделки бланков ценных бумаг и документов с определенной степенью защиты, документов с определенной степенью защиты, выпускаемых государством.

85 Сведения о лицах, содержащиеся в таможенных документах и статистических декларациях (периодических статистических декларациях). Описание товара, содержащееся в таможенных декларациях.

Банковская деятельность

86 Сведения об эскизных проектах, номинале (достоинстве), изображении, степени и элементах защиты, других характеристиках наличных денежных средств Республики Беларусь нового образца, эмитируемых Национальным банком, за исключением памятных банкнот (монет), слитковых (инвестиционных) монет, а также сведения об их производителях до официального опубликования в печати.

87 Сведения о плановых и фактических объемах производства и объемах выпуска в обращение наличных денежных средств Национального банка в натуральном и денежном выражении (за исключением памятных банкнот (монет) и слитковых (инвестиционных) монет).

88 Сведения о размерах запасов и местах хранения наличных денежных средств в белорусских рублях (за исключением памятных банкнот (монет) и слитковых (инвестиционных) монет) и иностранной валюте, а также о количестве иных ценностей (драгоценных металлов и камней, ценных бумаг, бланков ценных бумаг и документов с определенной степенью защиты и других), находящихся на хранении в структурных подразделениях Национального банка, банках и небанковских кредитно-финансовых организациях.

89 Сведения о расчете потребности экономики в наличных денежных средствах.

90 Сведения о работе служб Национального банка, банков и небанковских кредитно-финансовых организаций по инкассации и перевозке наличных денежных средств, платежных инструкций, драгоценных металлов, драгоценных камней и иных ценностей, оснащенности их оружием и другими техническими средствами защиты, а также о маршрутах перевозки ценностей и инкассации денежной наличности.

91 Сведения о деятельности Национального банка, связанной с конкретными операциями на валютном рынке, рынке драгоценных металлов и драгоценных камней.

92 Информация, получаемая в порядке банковского надзора, за исключением информации, подлежащей раскрытию в соответствии с законодательством Республики Беларусь.

93 Тестирующие телексные ключи для работы с иностранными банками.

94 Сведения о стратегии Национального банка во время очередных торгов в открытом акционерном обществе «Белорусская валютно-фондовая биржа».

95 Сведения о пропускном режиме и системе охраны, технической укрепленности, системах охранной, пожарной и тревожной сигнализации, видеонаблюдения, контроля и разграничения доступа в Национальном банке, банках и небанковских кредитно-финансовых организациях (кроме режимных объектов Национального банка).

96 Проектно-сметная документация на строительство и реконструкцию режимных объектов Национального банка (кроме наружных коммуникаций).

97 Сведения об организации автоматизированных вычислительных и информационных систем Национального банка, банков и небанковских кредитно-финансовых организаций, применяемых в этих системах организационных методах и программно-технических средствах защиты информации, включая сведения об организации администрирования и управления в вычислительных сетях.

98 Сведения об организации, методах и средствах комплексной защиты информации от несанкционированного доступа и утечки по техническим каналам, применяемых в Национальном банке, банках и небанковских кредитно-финансовых организациях.

Геодезия, картография

99 Государственные топографические карты масштабов 1 : 200 000 и 1 : 100 000, издательские оригиналы указанных карт в государственной системе геодезических координат 1995 года (СК-95) и в системах координат 1942 (СК-42) и 1963 (СК-63) годов, такие же материалы в масштабах 1 : 50 000 и крупнее, покрывающие площадь в одном массиве на территорию не более 4000 кв. километров, без географической и прямоугольной сеток и подписей их координат, номенклатуры трапеций, характеристик бродов и путепроводов, грузоподъемности мостов, а также специальные карты, созданные в установленном порядке на их основе, в графической, цифровой и иных формах и копии перечисленных материалов. Топографические планы масштабов 1 : 5000, 1 : 2000, 1 : 1000, 1 : 500, топографические планы населенных пунктов масштабов 1 : 25 000 и 1 : 10 000 в местных системах координат, специальные планы, созданные на их основе, в графической, цифровой и иных формах, а также копии перечисленных материалов.

100 Плановые координаты геодезических пунктов, определенные с точностью грубее 1 метра и до 50 метров включительно в СК-95 и в СК-42. Плановые координаты геодезических пунктов в СК-63 и местных системах координат, определенные с точностью 50 метров и точнее.

101 Аэроснимки (аэронегативы), репродукции накидного монтажа, фотопланы/ортофотопланы (кроме фотопланов (ортофотопланов), изготавливаемых и (или) используемых организациями Министерства обороны) и фотосхемы в масштабах 1 : 50 000 и крупнее в СК-95, СК-42, СК-63.

102 Технические проекты (задания, указания), исходные данные (ключи) систем координат и материалы, раскрывающие переход от одних систем

координат к другим, базы данных географических информационных систем, в том числе земельно-информационных систем, издания, фото-, кино-, видео- и аудиопленки, машинные и иные материальные носители, содержащие геодезическую и картографическую служебную информацию ограниченного распространения, перечисленную в пунктах 99–101 данного перечня.

Гидрометеорология

103 Координаты гидрометеорологических станций и постов, за исключением разрешенных для международного обмена гидрометеорологической информацией.

104 Сводные сведения об обеспечении гидрометеорологической информацией Вооруженных Сил Республики Беларусь, а также гидрометеорологические исследования и описания в интересах Вооруженных Сил Республики Беларусь.

Медико-санитарные вопросы

105 Сведения о новых медицинских средствах противорадиационной, противохимической и противобактериологической защиты войск, населения и животных.

106 Сведения об объемах производства наркотических средств, психотропных веществ и их прекурсоров, ввоза их в Республику Беларусь из конкретной страны и вывоза в конкретную страну.

107 Сведения о способе изготовления и применения наркотических средств, психотропных веществ и их прекурсоров.

108 Сведения о местах хранения наркотических средств, психотропных веществ, их прекурсоров и аналогов, ядов, радиоактивных веществ и сырья для их производства, маршруты их транспортировки.

109 Сведения о мобилизационных возможностях по заготовке донорской крови и ее препаратов (по областям и в целом по республике).

110 Сведения о мобилизационных мощностях по производству бактериальных препаратов, их запасах и поставках на военное время.

111 Сведения о разработке медицинского комплекта средств фармакологического обеспечения спортивной медицины и спорта высших достижений.

112 Сведения о фармакологическом обеспечении спортивной медицины и спорта высших достижений.

113 Сведения о разработке и внедрении лечебно-реабилитационных программ для спорта высших достижений.

Иные сведения

114 Иные сведения, касающиеся деятельности государственного органа, государственной организации, иного юридического лица, организации, не являющейся юридическим лицом, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц, организаций, не являющихся юридическими лицами.

ПРИЛОЖЕНИЕ Б

ФОРМА АКТА ОТНЕСЕНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ К КЛАССУ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

УТВЕРЖДАЮ

_____
(наименование должности

_____
руководителя организации)

_____
(подпись, инициалы, фамилия)

____.__.20__

АКТ
отнесения информационной системы к классу типовых информационных систем

_____
(наименование и место нахождения организации,

_____
полное наименование информационной системы)

Настоящий акт составлен комиссией, назначенной приказом ____.__.20__ г. №__, в составе:

председателя _____,

членов комиссии:_____

о том, что информационной системе _____
(полное наименование информационной системы)

в которой обрабатывается _____
(указывается наименование

_____ и которая
или конкретные виды информации и категория доступа к ней)

_____ к открытым каналам передачи данных,
подключена (не подключена)

присвоен класс _____

Председатель комиссии _____ _____
(подпись) (инициалы, фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы, фамилия)

_____ _____
(подпись) (инициалы, фамилия)

ПРИЛОЖЕНИЕ В

ДОПОЛНИТЕЛЬНЫЕ ОПЦИИ ПРОГРАММЫ

Таблица В.1 – Доступ к дополнительным опциям программы

Опция программы	Выбор опции программы	
	нажатием сочетания клавиш	с помощью меню
Получение методических указаний по выполнению задания	Ctrl + M	Учебный модуль → Методические указания по выполнению
Ознакомление с краткими теоретическими сведениями	–	Справка → Краткая теория → 1 Описание
Доступ к изучаемым схемам	–	Справка → Краткая теория → 2 Схемы
Ознакомление с формулами, используемыми для расчета контролируемых значений	–	Справка → Краткая теория → Расчетные формулы
Отмена загруженного учебного модуля	Ctrl + J	Учебный модуль → Отменить загруженный блок и выбрать …
Завершение выполнения учебного модуля	Alt + F4	Учебный модуль → Выход

ПРИЛОЖЕНИЕ Г

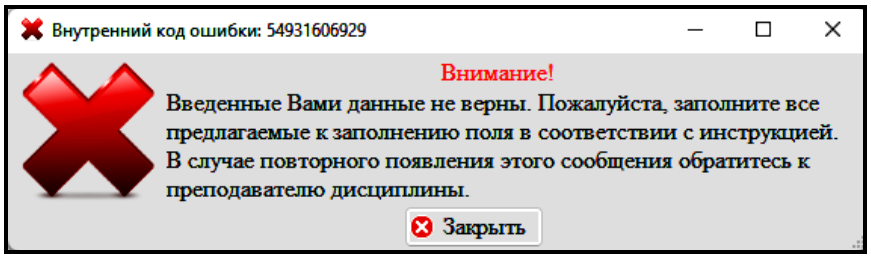
СВЕДЕНИЯ О ВОЗМОЖНЫХ СООБЩЕНИЯХ ПРОГРАММЫ

Таблица Г.1 – Сообщения об ошибках

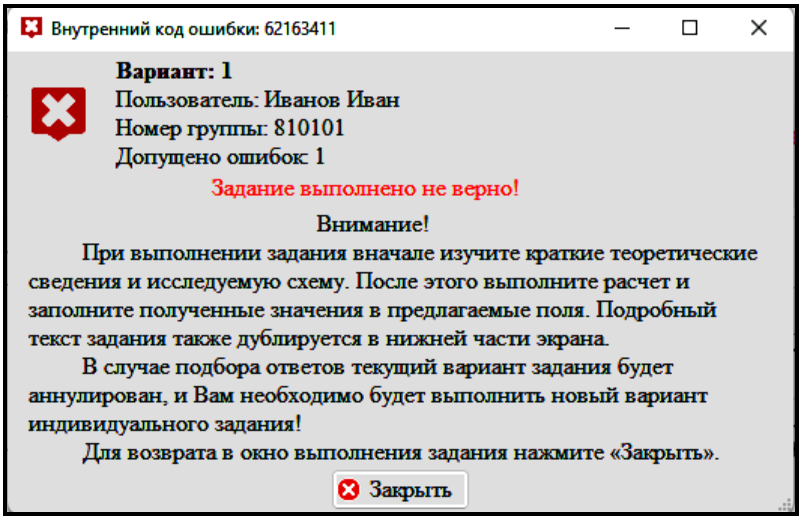
Код ошибки	Возможная причина	Устранение
54XXXXXXXXX	Данные введены некорректно	Заполните предлагаемые поля в соответствии с инструкцией для текущего окна
6XXXXXXX	Расчет по практическому заданию выполнен неверно	Пересчитайте контролируемые значения для заданного шага практического задания в соответствии с инструкцией для текущего окна и нажмите «Проверить»
17XXXXXX	Выбранное действие либо не может быть выполнено, либо может привести к сбою в работе программного обеспечения	Обратитесь к преподавателю учебной дисциплины

Примечание – Число X представлено в десятичной системе счисления и определяет тип ошибки и ее причину.

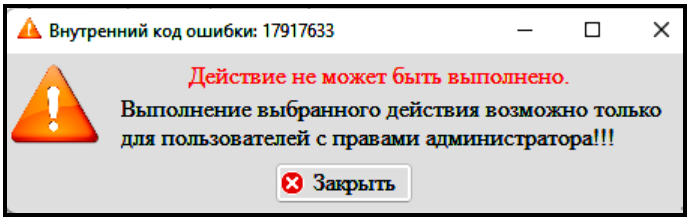
а



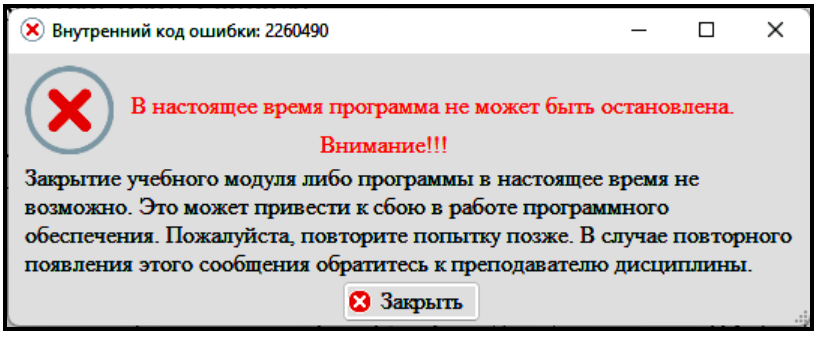
б



в



г



а – данные введены некорректно; *б* – расчет выполнен неверно; *в* – действие не может быть выполнено; *г* – действие может привести к сбою в работе программного обеспечения

Рисунок Г.1 – Примеры возможных сообщений об ошибках

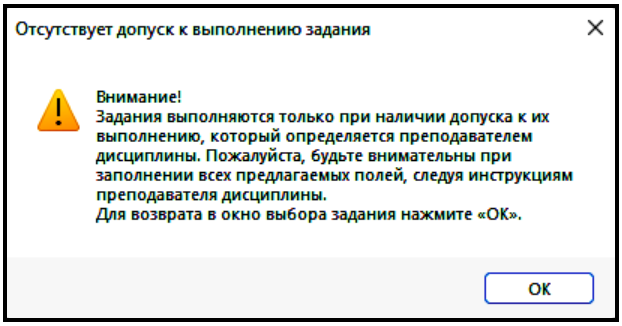


Рисунок Г.2 – Пример информационного сообщения

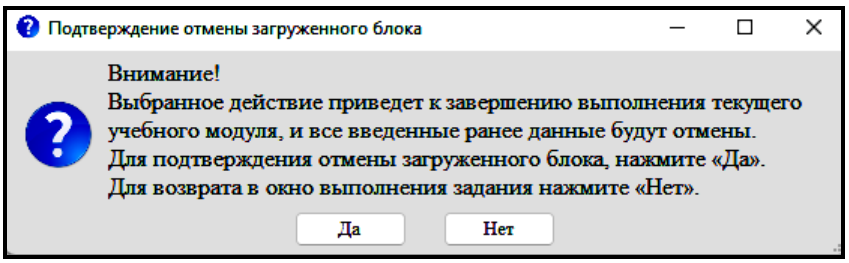


Рисунок Г.3 – Информационное сообщение
для подтверждения отмены загруженного блока

ПРИЛОЖЕНИЕ Д

ОБЯЗАТЕЛЬНЫЕ И РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАВИСИМОСТИ ОТ ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ И КЛАССОВ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Таблица Д.1 – Перечень требований к системе защиты информации, подлежащих включению в техническое задание на создание системы защиты информации [10]

Наименование требований	Типовой класс информационной системы									
	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	11
1. Аудит безопасности										
1.1 Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности, информация о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации и другое)	+	+	+	+	+	+	+	+	+	+
1.2 Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+	+	+
1.3 Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	±	±	+	±	±	+	+	+	±	+
1.4 Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы	+	+	+	+	+	+	+	+	+	+
1.5 Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+	+	+

Продолжение таблицы Д.1

1	2	3	4	5	6	7	8	9	10	11
2 Требования по обеспечению защиты данных										
2.1 Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием	+	+	+	+	+	+	+	+	+	+
2.2 Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации	+	+	+	+	+	+	+	+	+	+
2.3 Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности	+	+	+	+	+	+	+	+	+	+
3 Требования по обеспечению идентификации и аутентификации										
3.1 Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации	+	+	+	+	+	+	+	+	+	+
3.2 Обеспечение идентификации и аутентификации пользователей информационной системы	+	+	+	+	+	+	+	+	+	+
3.3 Обеспечение защиты обратной связи при вводе аутентификационной информации	+	+	+	+	+	+	+	±	+	+
3.4 Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы	+	+	+	+	+	+	+	+	+	+
3.5 Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы	+	+	+	+	+	+	+	+	+	+
3.6 Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы	±	±	±	±	±	±	±	+	+	+
3.7 Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу	+	+	+	+	+	+	+	+	+	+

Продолжение таблицы Д.1

1	2	3	4	5	6	7	8	9	10	11
4 Требования по защите системы защиты информации информационной системы										
4.1 Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию	+	+	+	+	+	+	+	+	+	+
4.2 Обеспечение обновления объектов информационной системы	+	+	+	+	+	+	+	+	+	+
4.3 Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы	+	+	+	+	+	+	+	+	+	+
4.4 Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации	+	+	+	+	+	+	+	+	+	+
5 Обеспечение криптографической защиты информации										
5.1 Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного шифрования), если не осуществлено предварительное шифрование защищаемой информации	±	±	±	±	±	+	+	+	+	+
5.2 Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)	±	±	+	±	±	±	±	+	±	±
5.3 Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)	+	+	+	+	+	+	+	+	+	+
5.4 Обеспечение контроля целостности данных в информационной системе (средства контроля целостности)	±	±	+	±	±	±	±	+	±	±
5.5 Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены)	±	±	±	±	+	±	±	±	±	+

Продолжение таблицы Д.1

1	2	3	4	5	6	7	8	9	10	11
5.6 Обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в информационной системе (криптографический токен и/или средства выработки электронной цифровой подписи)	±	±	±	±	±	±	±	±	±	±
6 Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре										
6.1 Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг	±	±	±	±	±	+	+	+	+	+
6.2 Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин	±	±	±	±	±	+	+	+	+	+
6.3 Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных	+	+	+	±	±	+	+	+	+	+
6.4 Обеспечение резервного копирования пользовательских виртуальных машин	±	±	+	±	+	+	+	+	+	+
6.5 Обеспечение резервирования сетевого оборудования по схеме N+1	±	±	±	±	±	±	±	±	+	+
6.6 Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	±	±	±	±	+	±	±	±	±	+
7 Иные требования										
7.1 Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	+	+	+	+	+	+	+	+	+	+
7.2 Обеспечение контроля за составом объектов информационной системы	+	+	+	+	+	+	+	+	+	+
7.3 Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования	±	±	±	±	±	±	±	+	+	+
7.4 Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы)	+	+	+	+	+	+	+	+	+	+
7.5 Определение состава и содержания информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+

Продолжение таблицы Д.1

1	2	3	4	5	6	7	8	9	10	11
7.6 Обеспечение резервирования информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+
7.7 Обеспечение резервирования конфигурационных файлов сетевого оборудования	±	±	+	±	+	+	+	+	+	+
7.8 Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления	+	+	+	+	+	+	+	+	+	+
7.9 Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных	±	±	±	±	±	±	±	+	+	+
7.10 Обеспечение защиты средств вычислительной техники от вредоносных программ	+	+	+	+	+	+	+	+	+	+
7.11 Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ	±	±	±	±	±	±	±	+	+	+
7.12 Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ	±	±	±	±	±	+	+	+	+	+
7.13 Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего)	±	±	±	±	±	+	+	+	+	+
7.14 Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях	±	±	±	±	±	+	+	+	+	+
7.15 Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях	±	±	±	±	±	+	+	+	+	+

Продолжение таблицы Д.1

1	2	3	4	5	6	7	8	9	10	11
7.16 Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений	±	±	±	±	±	+	+	+	+	+
7.17 Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений	±	±	±	±	±	+	+	+	+	+
7.18 Обеспечение обнаружения утечек информации из информационной системы. Использование системы обнаружения утечек информации из информационной системы	±	±	±	±	±	±	±	±	±	+
7.19 Определение перечня внешних подключений к информационной системе и порядка такого подключения	±	±	±	±	±	+	+	+	+	+
7.20 Обеспечение контроля за внешними подключениями к информационной системе	±	±	±	±	±	+	+	+	+	+
7.21 Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы	±	±	±	±	±	±	±	+	±	+

Примечание – Классы 5–14 соответствуют классам типовых информационных систем, приведенным в таблице 1 (см. практическое занятие 1); требования, отмеченные знаком «+», являются обязательными; требования, отмеченные знаком «±», являются рекомендуемыми.

ПРИЛОЖЕНИЕ Е

ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Таблица Е.1 – Требования к организации взаимодействия типовых информационных систем [10]

Классы	6-частн/ 6-гос	5-частн/ 5-гос	4-ин/4-спец/ 4-бг/4-юл/4-дсп	3-ин/3-спец/ 3-бг/3-юл/3-дсп
4-ин	х	не допускается	х	не допускается
4-спец	х	не допускается	х	не допускается
4-бг	х	не допускается	х	не допускается
4-юл	х	не допускается	х	не допускается
4-дсп	х	не допускается	х	не допускается
3-ин	не допускается	х/о	не допускается	х/о
3-спец	не допускается	х/о	не допускается	х/о
3-бг	не допускается	х/о	не допускается	х/о
3-юл	не допускается	х/о	не допускается	х/о
3-дсп	не допускается	х/о	не допускается	х/о

Примечания

1 Обозначения «3-ин», «3-спец», «3-бг», «3-юл», «3-дсп», «4-ин», «4-спец», «4-бг», «4-юл», «4-дсп», «5-частн», «5-гос», «6-частн» и «6-гос» соответствуют классам типовых информационных систем (см. практическое занятие 1).

2 Под символом «х» понимается физически выделенный канал передачи данных.

3 Под символом «о» понимается наличие подключения к открытым каналам передачи данных (в том числе к глобальной компьютерной сети Интернет).

ПРИЛОЖЕНИЕ Ж

МЕТОДЫ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 Для обезличивания персональных данных собственники (владельцы) информационных систем используют следующие методы:

– введение идентификаторов;

– изменение состава;

– декомпозиция;

– перестановка;

– зашифрование.

2 Метод введения идентификаторов реализуется путем замены персональных данных или части персональных данных, позволяющих идентифицировать субъекта персональных данных, их идентификаторами и создания таблицы соответствия с последующим раздельным хранением идентификаторов и таблиц.

3 Метод изменения состава реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта персональных данных, с последующим раздельным хранением полученных данных и правил изменения.

4 Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создания таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением подмножеств и таблиц.

Для реализации метода требуется предварительно разработать правила разбиения на подмножества, правила установления соответствия между записями в различных таблицах и правила внесения изменений в подмножества и таблицы.

5 Метод перестановки реализуется путем взаимного перемещения отдельных записей, а также групп записей между собой с последующим раздельным хранением полученных данных и правил изменения.

6 Метод зашифрования реализуется путем применения средств криптографической защиты информации (предварительного шифрования), имеющих сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Тимофеев, А. М. Симметричные криптосистемы: стандарт DES. Лабораторный практикум : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2024. – 123 с.

2 Левашов, П. Киберкрепость: всестороннее руководство по компьютерной безопасности / П. Левашов. – СПб. : Питер, 2024. – 544 с.

3 Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз. – М. : ДМК Пресс, 2020. – 308 с.

4 Щеглов, А. Ю. Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам: методы, модели, технические решения / А. Ю. Щеглов. – СПб. : Профессиональная литература, 2017. – 416 с.

5 О государственных секретах : Закон Респ. Беларусь от 19 июля 2010 г. № 170-З [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=2012&oldDoc=2010-184/2010-184(014-064).pdf&oldDocPage=9. – Дата доступа: 01.09.2024.

6 О защите персональных данных : Закон Респ. Беларусь от 7 мая 2021 г. № 99-З [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099. – Дата доступа: 01.09.2024.

7 О коммерческой тайне : Закон Респ. Беларусь от 5 января 2013 г. № 16-З [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H11300016. – Дата доступа: 01.09.2024.

8 О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну : Постановление Совета Министров Респ. Беларусь от 12 августа 2014 г. № 783 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=C21400783. – Дата доступа: 01.09.2024.

9 Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=2012&oldDoc=2008-279/2008-279(014-027).pdf&oldDocPage=1. – Дата доступа: 01.09.2024.

10 О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 : Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 20 февраля 2020 г. № 66 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf. – Дата доступа: 01.09.2024.

11 Деятельность ОАЦ в сфере кибербезопасности и защита информации. Техническая и криптографическая защита информации. Средства защиты информации. Общие сведения [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/activity/information-security-tools/technical-and-cryptographic-information-protection/general-information. – Дата доступа: 01.09.2024.

12 Деятельность ОАЦ в сфере кибербезопасности и защита информации. Техническая и криптографическая защита информации. Средства защиты информации. Реестр средств защиты информации, прошедших экспертизу [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/activity/information-security-tools/technical-and-cryptographic-information-protection/register-of-information-security-tools-that-have-passed-the-examination. – Дата доступа: 01.09.2024.

13 Деятельность ОАЦ в сфере кибербезопасности и защита информации. Техническая и криптографическая защита информации. Средства защиты информации. Реестр средств защиты информации, прошедших сертификацию [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/activity/information-security-tools/technical-and-cryptographic-information-protection/registry-ism. – Дата доступа: 01.09.2024.

14 Тимофеев, А. М. Лицензирование деятельности в сфере защиты информации : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2021. – 118 с.

15 О лицензировании : Закон Респ. Беларусь от 14 октября 2022 г. № 213-З [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3961&p0=H12200213. – Дата доступа: 01.09.2024.

16 О лицензировании отдельных видов деятельности : Указ Президента Респ. Беларусь от 1 сентября 2010 г. № 450 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=2012&oldDoc=2010-212/2010-212(003-097).pdf&oldDocPage=3. – Дата доступа: 01.09.2024.

17 Деятельность ОАЦ в сфере кибербезопасности и защита информации. Техническая и криптографическая защита информации. Лицензирование [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/activity/technical-and-cryptographic-information-protection/licensing. – Дата доступа: 01.09.2024.

Св. план 2025, поз. 29

Учебное издание

Тимофеев Александр Михайлович

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ. ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИТЫ ДЛЯ ТИПОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *А. Ю. Шурко*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *А. А. Лущикова*

Подписано в печать 25.04.2025. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 7,21. Уч.-изд. л. 6,2. Тираж 50 экз. Заказ 1.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск