ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ, УСТАНОВКЕ, НАЛАДКЕ, ЭКСПЛУАТАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

СТ РК 34.022-2006

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «Гранит»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 15 декабря 2006 г. № 550

3 В настоящем стандарте учтены основные нормативные положения следующих международных документов: Рекомендации ИСО/МЭК 15408-1:2005 Технологии информационные. Методы защиты. Критерии оценки защиты информационных технологий. Часть 1. Введение и общая модель. Рекомендации ИСО/МЭК 15408-2:2005 Технологии информационные. Методы защиты. Критерии для оценки защиты информационных технологий. Часть 2. Эксплуатационные требования безопасности. Рекомендации ИСО/МЭК 15408-3:2005 Технологии информационные Методы защиты. Критерии для оценки защиты информационных технологий. Часть 3. Требования к обеспечению защиты

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2011 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Защита информации

ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ, УСТАНОВКЕ, НАЛАДКЕ, ЭКСПЛУАТАЦИИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Дата введения 2008.01.01

1 Область применения

Настоящий стандарт распространяется на информационные системы, используемые в различных видах деятельности, в процессе создания и применения которых осуществляется обработка защищаемой информации, содержащей сведения, отнесенные к государственным секретам [1].

Настоящий стандарт устанавливает порядок разработки, внедрения и эксплуатации информационных систем, отвечающих требованиям информационной безопасности.

Настоящий стандарт применяется в средствах криптографической защиты для повышения гарантий качества защиты информации.

Положения настоящего стандарта подлежат применению государственными органами и организациями Республики Казахстан, взявшими на себя обязательства либо обязанными по статусу выполнять требования правовых документов по защите информации.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 34.005-2002 Информационная технология. Основные термины и определения.

СТ РК 34.013-2002 Информационная технология. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок при ее обработке на средствах вычислительной техники.

СТ РК 1171-2002 Защита информации. Типовая методика контроля эффективности защиты служебных помещений от акустической разведки по акустическому (речевому) и вибрационному каналам.

СТ РК 1200-2002 Государственная система защиты информации. Технические средства защиты информации, используемые в государственных учреждениях. Технические требования.

СТ РК 1201-2002 Государственная система защиты информации. Порядок разработки, согласования, утверждения и государственной регистрации средств защиты информации.

СТ РК 1202-2002 Государственная система защиты информации. Общие требования к техническим средствам защиты информации. Основные положения.

ГОСТ 2.119-73 ЕСКД. Эскизный проект.

ГОСТ 2.120-73 ЕСКД. Технический проект.

ГОСТ 2.601-95 ЕСКД. Эксплуатационные документы.

ГОСТ 21552-84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение

Издание официальное

ГОСТ 23773-88 Машины вычислительные электронные цифровые общего назначения. Методы испытаний.

3 Термины и определения

В настоящем стандарте применены термины с соответствующими определениями, установленные в СТ РК 34.005, а также следующие:

3.1 **Заказчик:** Юридическое лицо (государственное орган или организация независимо от формы собственности), формулирующее требования к ИС, финансирующее работы по ее созданию или по заказам которого осуществляется создание (развитие) и обслуживание ИС.

3.2 **Информационная система:** Система обработки информации совместно с соответствующими организационными ресурсами, такими как человеческие, технические и финансовые ресурсы, предоставляющая и распределяющая информацию.

3.3 **Государственные секреты:** Защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.

3.4 **Государственная тайна:** Сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан.

3.5 **Служебная тайна:** Сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.

3.6 **Защищаемая информация:** Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

3.7 **Объект информатизации:** Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, в которых они установлены.

3.8 **Информационная безопасность:** Защищенность информации и оборудования ИС от факторов, представляющих угрозу для конфиденциальности (обеспечение санкционированного доступа), целостности и доступности.

3.9 **Анализ рисков:** Процесс определения угроз безопасности ИС и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также контрмер.

3.10 **Угрозы информационной безопасности:** Совокупность причин, условий и факторов, создающих опасность объектам информационной безопасности, реализация которых может повлечь нарушение прав, свобод и законных интересов юридических и физических лиц в информационных процессах.

3.11 **Фактор, воздействующий на защищаемую информацию:** Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации или блокирование доступа к ней.

3.12 **Несанкционированное воздействие на информацию:** Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа,

приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

3.13 **Непреднамеренное воздействие на информацию:** Ошибка пользователя информацией, сбой технических и программных средств, ИС, а также природные явления или иное нецеленаправленное на изменение информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования ее носителя.

3.14 **Политика информационной безопасности:** Совокупность документов, определяющих управленческие и проектные решения в области информационной безопасности.

3.15 **Профиль защиты:** Документ, описывающий задачи обеспечения ИБ в терминах функциональных требований и требований гарантированности.

3.16 **Гарантированность механизмов обеспечения ИБ:** Оценка адекватности используемых механизмов обеспечения ИБ выбранным функциональным требованиям. Гарантированность определяется эффективностью и корректностью механизмов обеспечения ИБ.

3.17 **Техническое задание:** Документ, используемый заказчиком в качестве средства для описания и определения задач, выполняемых при реализации договора.

3.18 **Пользователь:** Некто или нечто, посылающий команды и сообщения в ИС и получающий информацию от нее. Пользователями могут быть машины или другие системы, а также люди.

3.19 **Методическое обеспечение ИС:** Документы, которые отражают взаимодействие пользователя с комплексом средств информатизации, включая описание системы и подсистем, методику (технологию) выполнения автоматизированной деятельности, инструкций пользователей.

3.20 **Организационное обеспечение ИС:** Документы (положения, должностные инструкции, штатные расписания, квалификационные требования и др.), устанавливающие организационную структуру, функции и порядок взаимодействия между собой подразделений при работе ИС, в том числе инструкции персоналу.

3.21 **Компонент ИС:** Элемент одного из видов обеспечения (технического, программного, информационного и др.), выполняющий определенную функцию в подсистеме ИС и обеспечивающий ее работу.

3.22 **Оборудование информационных технологий:** Любое оборудование, выполняющее функцию, связанную с вводом, хранением, отображением, поиском, передачей, обработкой, управлением или коммутацией данных и сообщений связи.

3.23 **Режимные помещения:** Помещения, в которых проводятся секретные работы, хранятся секретные документы и изделия, циркулирует иная секретная информация, а также установлены технические средства, предназначенные для ее обработки.

3.24 **Основные технические средства:** Средства вычислительной техники, средства связи, звукозаписи, звукоусиления и звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционная аппаратура, системы электрооборудования и другие средства и системы, используемые для обработки секретной информации или не используемые для обработки секретной информации, но находящиеся в режимных помещениях.

3.25 **Вспомогательные технические средства:** Технические средства, непосредственно не участвующие в обработке секретной информации, но используемые совместно с основными техническими средствами и находящиеся в зоне электромагнитного поля основных технических средств.

4 Обозначения и сокращения

В настоящем стандарте применены обозначения и сокращения:
ИБ – информационная безопасность;
ИС – информационная система;
ЗИ – защита информации;
ТЗ – техническое задание;
ТТЗ – тактико-техническое задание;
НИР – научно-исследовательская работа;
ОКР - опытно-конструкторская работа;
ПЭМИН – побочные электромагнитные излучения и наводки;
СНиП - строительные нормы и правила.

5 Общие положения

5.1 Целесообразность создания и внедрения ИС определяется социальными, научно-техническими или другими полезными эффектами, получаемыми в результате ввода в эксплуатацию ИС.

5.2 Проектирование (модернизация) и внедрение ИС проводится, как правило, в рамках ОКР. Функции основных участников ОКР, взаимоотношения между ними, правила выполнения и порядок реализации законченной ОКР определены СТ РК 1201.

5.3 Проектирование и внедрение вновь создаваемой (модернизируемой) ИС производится в соответствии с ТЗ. ТЗ на ИС является основным документом, определяющим требования, предъявляемые к ИС, порядок создания (модернизации) и приемку при вводе в эксплуатацию.

5.4 В процессе проектирования (модернизации), монтажа и эксплуатации ИС должна быть организована разрешительная система доступа разработчиков, специалистов по монтажу и наладке, пользователей, обслуживающего и эксплуатирующего персонала к техническим, программным средствам и информационным ресурсам ИС. Перечисленные группы специалистов должны иметь допуск к государственным секретам по соответствующей форме.

5.5 Полномочия разработчиков, пользователей, обслуживающего и эксплуатирующего персонала по доступу к ресурсам ИС устанавливаются заказчиком.

5.6 Заказчик, собственник (владелец) ИС, а также организации-участники создания ИС несут ответственность за обеспечение защиты обрабатываемой в ИС информации и выполнение работ по ЗИ на всех стадиях создания и эксплуатации ИС.

5.7 Организации – участники работ по созданию ИС должны иметь лицензию на право проведения работ в области защиты информации. Лицензирование организаций осуществляется в установленном порядке [1].

5.8 Для создания ИС могут применяться как серийно выпускаемые, так и вновь разработанные технические и программные средства обработки информации, а также технические, программные, программно-технические, криптографические средства защиты информации и средства для контроля эффективности ЗИ. Применяемые средства должны иметь сертификаты соответствия по требованиям безопасности информации, выдаваемые соответствующими органами по подтверждению соответствия.

Вновь разработанные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации ИС.

5.9 Прекращение эксплуатации ИС предусматривается по следующим основаниям:

- по решению собственника (владельца) ИС, оформленному в установленном порядке;

- согласно принятому решению органа надзора (контроля) из-за несоответствия требованиям нормативных документов по защите информации или другим причинам, приводящим к утечке или другим угрозам защищаемой информации;
- по решению суда.

6 Проектирование информационных систем

6.1 Стадии и этапы создания ИС

Процесс создания ИС представляет собой совокупность работ, упорядоченных во времени, взаимно связанных, объединенных в стадии и этапы. Стадии и этапы создания ИС приведены в таблице 1.

Таблица 1 – Стадии и этапы создания ИС

Стадия создания ИС	Этапы работ
1 Формирование требований к ИС	1.1 Обследование объекта и обоснование необходимости создания ИС. 1.2 Формирование исходных требований заказчика к ИС. 1.3 Оформление отчета о выполненной работе и заявки на разработку ИС.
2 Разработка концепции ИС и концепции ИБ	2.1 Изучение объекта информатизации. 2.2 Проведение НИР (при необходимости). 2.3 Разработка вариантов концепции ИС и вариантов концепции ИБ, выбор варианта концепции ИС и варианта концепции ИБ, удовлетворяющих требованиям заказчика. 2.4 Разработка технического (тактико-технического) задания на аванпроект. 2.5 Оформление отчета о выполненной работе. 2.6 Оформление совместного решения заказчика и исполнителя на разработку аванпроекта.
3 Аванпроект	3.1 Разработка ТЗ на ИС в целом. 3.2 Разработка частных ТЗ на подсистемы ИС.
4 Эскизный проект	4.1 Разработка предварительных проектных решений по выбранному варианту ИС, реализующие механизмы функционирования. 4.2 Разработка документации на ИС и ее части.
5 Технический проект	5.1 Разработка проектных решений по системе и ее компонентам. 5.2 Разработка документации на ИС и ее части. 5.3 Разработка и оформление документов на комплектующие изделия и/или технических заданий (технических требований) на их разработку. 5.4 Разработка заданий на проектирование в смежных частях проекта объекта информатизации.
6 Рабочая документация	6.1 Разработка рабочей документации на ИС и ее компоненты. 6.2 Разработка или адаптация программ.

Окончание таблицы 1

Стадия создания ИС	Этапы работ
7 Ввод в действие	7.1 Подготовка объекта информатизации к вводу ИС в действие. 7.2 Подготовка персонала. 7.3 Комплектация ИС поставляемыми изделиями. 7.4 Строительно-монтажные работы. 7.5 Пусконаладочные работы. 7.6 Проведение предварительных испытаний. 7.7 Проведение опытной эксплуатации. 7.8 Проведение приемочных испытаний.
8 Эксплуатация ИС	8.1 Выполнение работ в соответствии с гарантийными обязательствами. 8.2 Эксплуатация ИС.

6.1.1 Состав, последовательность и сроки реализации стадий и этапов работ, выполняемых при создании (развитии) ИС устанавливают в техническом задании (или в ведомости исполнения договора) на создание (развитие) системы из числа стадий и этапов работ, приведенных в настоящем стандарте.

6.1.2 В зависимости от специфики создаваемой ИС и условий ее создания допускается выполнять отдельные этапы работ до завершения предшествующих стадий и параллельное во времени выполнение этапов работ.

6.1.3 Техническое задание и проектно-сметная документация на разработку ИС в обязательном порядке согласовывается с уполномоченным государственным органом по защите государственных секретов и информационной безопасности, уполномоченными органами в сфере информации и связи и обеспечения национальной безопасности.

6.2 Содержание работ по этапам проектирования

6.2.1 На этапе 1.1 «Обследование объекта и обоснование необходимости создания ИС» в общем случае предусматривается выполнение следующих работ:

- обследование (сбор сведений и анализ) объекта информатизации, оценка состояния режима информационной безопасности (ИБ);
- формулировка требований по обеспечению режима ИБ при реализации функций и задач проектируемой ИС;
- сбор сведений о зарубежных и отечественных аналогах;
- оценку технико-экономической, социальной и т. п. целесообразности создания ИС.

6.2.2 На этапе 1.2 «Формирование исходных требований заказчика к ИС» проводят подготовку исходных данных для формирования требований к ИС:

- характеристику объекта информатизации;
- функции и задачи создаваемой ИС;
- условия функционирования ИС (требования к климатическим и механическим воздействиям);
- требования к обеспечению режима ИБ по каждой функции и задаче ИС (период недоступности, время доступа и другие показатели, определяемые предметной областью; показатели надежности, хранения, доставки; градации конфиденциальности информации);
- условия создания и эксплуатации ИС;
- ограничение допустимых затрат на разработку;

- проведение НИР (при необходимости);
- формулировку и оформление требований к ИС.

6.2.3 На этапе 1.3 «Оформление отчета о выполненной работе и заявки на разработку ИС» проводят оформление отчета о выполненных работах на данном этапе и оформляют заявку на разработку ИС или другого заменяющего ее документа.

6.2.4 На этапах 2.1 «Изучение объекта информатизации» и 2.2 «Проведение НИР» организация – исполнитель НИР проводит детальное исследование объекта информатизации и необходимые НИР, связанные с поиском путей и оценкой возможности реализации требований заказчика, оформляют и утверждают отчеты по проведенным НИР.

6.2.5 На этапе 2.3 «Разработка вариантов концепции ИС и концепции ИБ, выбор варианта концепции ИС и варианта концепции ИБ, удовлетворяющих требованиям заказчика» проводят:

- анализ правовых и договорных требований;
- разработку альтернативных вариантов концепции ИС, альтернативных вариантов концепции ИБ и планов их реализации;
- анализ угроз (классы рисков) которым могут подвергаться информационные ресурсы системы;
- оценку необходимых ресурсов на реализацию альтернативных вариантов и обеспечение функционирования;
- оценку преимуществ и недостатков каждого из вариантов;
- сопоставление требований заказчика и характеристик предлагаемого варианта ИС;
- выбор оптимального варианта концепции ИС и выбор оптимального варианта концепции ИБ;
- определение порядка оценки качества и условий приемки ИС;
- оценку эффектов, получаемых от ИС.

6.2.6 На этапе 2.4 «Разработка технического (тактико-технического) задания на аванпроект» проводится разработка, согласование и утверждение ТЗ (ТТЗ) на аванпроект и, при необходимости, технические задания на составные части ИС.

6.2.7 На этапе 2.5 «Оформление отчета о выполненной работе» подготавливается и оформляется отчет, содержащий описание выполненных работ на стадии, описание и обоснование предлагаемого варианта концепции ИС и предлагаемого варианта концепции ИБ.

6.2.8 На этапе 2.6 «Оформление совместного решения заказчика и исполнителя на разработку аванпроекта» заключается договор или оформляется совместное решение заказчика и исполнителя на разработку аванпроекта.

6.2.9 Этап 3.1 «Разработка ТЗ на ИС» и этап 3.2 «Разработка частных ТЗ на подсистемы ИС» предусматривает выполнение работ 6.2.9.1 – 6.2.9.8

6.2.9.1 Техническое обоснование целесообразности создания ИС, проработка вопросов ее применения.

6.2.9.2 Определение технических возможностей, путей создания ИС, рассмотрение возможных вариантов технических решений, обоснование выбора оптимального варианта и состава ИС.

6.2.9.3 Формирование требований к ИС:

- общие технические требования;
- требования к функциям ИС;
- требования к техническому обеспечению;
- требования к программному обеспечению;
- требования к информационному обеспечению;
- требования к лингвистическому обеспечению;

- требования к организационному обеспечению;
- требования к методическому обеспечению;
- описание угроз информации;
- задачи защиты информации в ИС;
- перечень защищаемой информации и требуемые нормы (уровни) эффективности ее защиты;
- выбор элементов системы, для которых будет производиться анализ рисков;
- профиль защиты и требования к средствам ЗИ;
- требования к обеспечению режима ИБ;
- требования по обеспечению бесперебойной работы организации;
- требования к подготовленности персонала;
- требование к правовому обеспечению;
- требования к документации.

6.2.9.4 Сопоставление проектируемой ИС с аналогичными отечественными и зарубежными образцами по показателям, согласованным с заказчиком.

6.2.9.5 Определение образцов компонентов ИС для проведения испытаний.

6.2.9.6 Расчет лимитной стоимости выполнения ОКР и ориентировочных затрат на эксплуатацию ИС.

6.2.9.7 Разработка ТЗ на ОКР по созданию ИС.

6.2.9.8 Составление отчетной документации по результатам выполнения аванпроекта с обоснованием принимаемых по нему решений.

6.2.10 Стадия «Эскизный проект» предусматривает выполнение этапов работ 4.1 и 4.2 на этапе разработки эскизного проекта ОКР.

6.2.10.1 На этапе 4.1 «Разработка предварительных проектных решений по выбранному варианту ИС, реализующие механизмы функционирования» определяются:

- функции ИС;
- функции подсистем, их цели и эффекты;
- состав комплексов задач и отдельных задач;
- концепция информационной базы, ее укрупненная структура;
- функции системы управления базой данных и состав вычислительной системы;
- функции и параметры основных программных средств;
- технические решения по структуре системы и подсистем, обеспечивающих режим ИБ, уровни иерархии и система управления ИБ;
- технические решения по режимам функционирования и диагностике состояний системы, обеспечивающей режим ИБ;
- описание показателей, характеризующих качество системы, обеспечивающих режим ИБ и методы их измерения;
- перечень угроз ИБ, для которых обеспечивается защита в рамках предлагаемого проектного решения.

6.2.10.2 На этапе 4.2 «Разработка документации на ИС и ее части» проводят разработку, оформление, согласование и утверждение документации в объеме, необходимом для описания полной совокупности принятых решений и достаточном для дальнейшего выполнения работ по созданию ИС.

В пояснительной записке приводится обоснование выбора технических средств обеспечивающих в пусковом, нормальном и аварийных режимах функционирование информационной системы и технических средств ЗИ и режим ИБ.

6.2.11 Стадия «Технический проект» реализуется на этапе разработки технического проекта ОКР и включает в себя этапы 5.1 – 5.4.

6.2.11.1 На этапе 5.1 «Разработка проектных решений по системе и ее компонентам» обеспечивают разработку общих решений по ИС и ее частям, функционально –

алгоритмической структуре системы, по функциям персонала и организационной структуре, по структуре технических средств, по алгоритмам решений задач и применяемым языкам, по организации и ведению информационной базы, по программному обеспечению, по организации сбора и передачи данных.

6.2.11.2 На этапе 5.2 «Разработка документации на ИС и ее части» производится разработка окончательных решений по общесистемным вопросам, в том числе по структурам ИС и по видам обеспечения.

В части ИБ на этапе должны быть разработаны:

- должностные инструкции персонала, регламентирующие вопросы доступа в помещения и к оборудованию, работу с носителями информации, доступ к информации;
- правила администрирования в ИС;
- правила работы пользователей в ИС;
- правила работы со сторонними организациями.

Должен быть разработан план мероприятий по обеспечению режима ИБ с рассмотрением основных составляющих комплексной системы защиты:

- организация работы персонала;
- физическая защита и контроль соблюдения режима ИБ;
- организация доступа в многопользовательской системе;
- поддержание работоспособности и обеспечение ИБ в сетях;
- планирование восстановительных работ.

Результаты работы должны быть изложены в техническом проекте «Средства защиты информации и средства контроля эффективности защиты» как разделе технического проекта ИС.

6.2.11.3 На этапе 5.3 «Разработка и оформление документов на комплектующие изделия и/или технических заданий (технических требований) на их разработку» проводят:

- подготовку и оформление документации на поставку изделий для комплектования ИС;
- определение технических требований и составление ТЗ на разработку изделий, не поставляемых серийно;
- разработку технических заданий на средства защиты информации и изготовление опытных образцов;
- разработку технических заданий на средства контроля эффективности защиты информации и изготовление опытных образцов.

6.2.11.4 На этапе 5.4 «Разработка заданий на проектирование в смежных частях проекта объекта информатизации» осуществляют разработку, оформление, согласование и утверждение заданий на проектирование в смежных частях проекта ИС для проведения строительных, электротехнических, коммуникационных, санитарно-технических и других подготовительных работ, связанных с созданием ИС.

6.2.12 На этапе 6.1 «Разработка рабочей документации на ИС и ее компоненты» проводят разработку рабочей документации, содержащей все необходимые и достаточные сведения для обеспечения выполнения работ по вводу ИС в действие и ее эксплуатацию, а также для поддержания уровня эксплуатационных характеристик системы в соответствии с принятыми проектными решениями, ее оформление, согласование и утверждение.

Должен быть разработан план мероприятий по обеспечению режима ИБ, содержащий разделы:

- организация работы персонала;
- физическая защита ИС и контроль соблюдения ИБ;
- организация доступа в многопользовательской системе;

- поддержание работоспособности и обеспечение ИБ в сетях;
- планирование восстановительных работ.

Должны быть разработаны:

- должностные инструкции персонала, регламентирующие вопросы доступа в помещения и к оборудованию, работу с носителями информации, доступ к информации, уничтожение носителей информации;
- правила администрирования в ИС;
- правила работы пользователей в ИС;
- правила работы со сторонними организациями.

Также на этом этапе должны быть изготовлены опытные образцы компонентов, изготовленных по ТЗ в рамках конкретной ОКР на ИС и проведены их испытания.

На этапе 6.2 «Разработка или адаптация программ» проводят разработку программ и программных средств системы, выбор, адаптацию и/или привязку приобретаемых средств, подтверждение соответствия приобретенных программных средств установленным требованиям информационной безопасности, проводимое соответствующими аккредитованными органами по подтверждению соответствия.

Должны быть приведены технические решения по организации сбора и передачи данных, а также технические решения по программному обеспечению, относящиеся к режиму ИБ.

6.2.13 На этапе 7.1 «Подготовка объекта информатизации к вводу ИС в действие» проводят работы по организационной подготовке объекта информатизации к вводу ИС в действие, в том числе:

- реализацию проектных решений по организационной структуре ИС;
- обеспечение подразделений инструктивно-методическими материалами;
- внедрение классификаторов информации;
- выявление критически важных функций и систем, определяющих ИБ в ИС;
- определение перечня возможных аварий и их последствий для ИБ;
- разработка мер ИБ, направленных на ликвидацию последствий нарушений в работе, вызванных стихийными бедствиями, авариями, атаками нарушителей.

В многопользовательской системе также должны быть решены вопросы доступа в ИС:

- регистрация пользователей;
- управление паролями пользователей;
- управление привилегиями;
- пересмотр прав доступа пользователей;
- управление привилегированным доступом для администрирования системы, в том числе системы ИБ.

В процессе подготовки к эксплуатации должна быть организована физическая защита объекта информатизации и организован контроль соблюдения режима ИБ в части вопросов:

- доступ в помещения;
- сохранение конфиденциальности;
- ведение журналов регистрации событий - учет попыток доступа (успешных и неудачных) в ИС;
- организация доступа к носителям информации и их защите (регистрация пользователей, управление привилегиями; управление пользовательскими паролями; пересмотр прав доступа пользователей; отслеживание времени простоя терминалов и защита пользовательского оборудования, оставленного без присмотра; ограничение доступа к сервисам; ограничение допустимого периода подключения);
- доступ к документации по ИС.

На этапе 7.2 «Подготовка персонала» проводят обучение персонала и проверку его подготовленности обеспечить функционирование ИС, а также должны быть решены вопросы доступа пользователей к работе в ИС, организации физической защиты и контроля за соблюдением режима ИБ.

На этапе 7.3 «Комплектация ИС поставляемыми изделиями» обеспечивают получение комплектующих изделий серийного и единичного производства, материалов и монтажных изделий. Проводится входной контроль их качества и подтверждение соответствия установленным требованиям информационной безопасности.

На этапе 7.4 «Строительно-монтажные работы» проводят:

- выполнение работ по строительству специализированных помещений (зданий, сооружений) для размещения технических средств и персонала ИС;
- сооружение кабельных каналов;
- выполнение работ по монтажу технических средств и линий связи;
- испытание смонтированных технических средств;
- сдачу смонтированных технических средств для проведения пусконаладочных работ.

На этапе 7.5 «Пусконаладочные работы» проводят автономную отладку технических и программных средств, загрузку информации в базу данных и проверку системы ее ведения, комплексную наладку всех средств системы. В процессе проведения работ должен быть организован контроль:

- доступа в помещения;
- сохранения конфиденциальности;
- ведения журналов регистрации событий;
- организации доступа к носителям информации;
- доступа к документации по ИС.

Пусконаладочные работы должны проводиться с применением несекретной (условной) информации.

На этапе 7.6 «Проведение предварительных испытаний» осуществляют:

- испытания ИС на работоспособность и соответствие техническому заданию в соответствии с программой и методикой предварительных испытаний;
- проверку реагирования ИС на чрезвычайные ситуации и переход на аварийный режим работы;
- проверку программно-технических механизмов ИБ во всех режимах работы ИС при выполнении функций и решении контрольных задач;
- устранение неисправностей и внесение изменений в конструкторскую документацию на ИС;
- оформление протоколов испытаний и акта о приемке ИС в опытную эксплуатацию.

На этапе 7.7 «Проведение опытной эксплуатации» проводят:

- опытную эксплуатацию ИС;
- анализ результатов опытной эксплуатации;
- доработку (при необходимости) программного обеспечения ИС, средств защиты информации и средств контроля эффективности защиты информации;
- комплексную отладку технических средств ЗИ во всех режимах работы, включая аварийные режимы ИС;
- оформление акта о завершении опытной эксплуатации ИС.

На этапе 7.8 «Проведение приемочных испытаний» проводят:

- проведение испытаний на соответствие ТЗ в соответствии с утвержденной в установленном порядке программой и методикой приемочных испытаний;
- анализ результатов испытаний и устранение недостатков, выявленных в процессе испытаний;

- оформление протоколов испытаний и акта о приемке ИС в эксплуатацию;
- приемку разработанной ИС администратором бюджетной программы в установленном законодательством порядке;
- проведение отраслевой оценки ИС уполномоченным органом в сфере информатизации и связи в соответствии с нормативными правовыми актами.

Датой ввода ИС в эксплуатацию считают дату подписания акта о вводе ИС в действие приемочной комиссией.

Применение ИС для обработки защищаемой информации разрешается только после подтверждения ее соответствия установленным требованиям безопасности информации, проводимое соответствующими аккредитованными органами по подтверждению соответствия.

Решение о возможности применения ИС принимает заказчик на основании акта комиссии по проведению приемочных испытаний системы.

6.2.14 На этапе 8.1 «Выполнение работ в соответствии с гарантийными обязательствами» осуществляют работы по устранению недостатков, выявленных при эксплуатации ИС в течение установленных гарантийных сроков, внесению необходимых изменений в документацию на ИС.

На этапе 8.2 «Эксплуатация ИС» осуществляют работы по:

- анализу функционирования ИС;
- выявлению отклонений фактических эксплуатационных характеристик от проектных значений и установлению причин этих отклонений;
- устранению выявленных недостатков и обеспечению стабильности эксплуатационных характеристик и ИБ;
- внесению изменений в конструкторскую документацию в соответствии с утвержденными процедурами и правилами доведения внесенных изменений до сведения лиц, которых они затрагивают.

6.3 Результаты выполнения работ по стадиям

6.3.1 Результатом выполнения стадии «Формирование требований к ИС» являются научно-технический отчет, техническое задание на аванпроект, технико-экономическое обоснование и заявка на создание ИС.

6.3.2 Результатом выполнения стадии «Разработка концепции ИС и концепции ИБ» является отчет. В отчете, разрабатываемом на этой стадии, в разделе «Функции и задачи создаваемой ИС» должен присутствовать подраздел «Требования к обеспечению режима ИБ». В нем должны быть описаны требования к обеспечению режима ИБ по каждой функции и задаче ИС.

После выбора варианта концепции создаваемой ИС должна быть разработана концепция ИБ на основе анализа следующих групп факторов:

- правовые и договорные требования;
- требования к обеспечению режима ИБ по функциям и задачам ИС;

По результатам анализа формулируются общие положения ИБ, затрагивающие организацию в целом:

- цели и приоритеты, которые преследует организация в области ИБ;
- общие направления в достижении этих целей;
- аспекты программы ИБ, которые должны решаться на уровне организации в целом;
- должностные лица и их обязанности по реализации программы ИБ.

Концепция политики ИБ должна быть оформлена в виде отчета.

6.3.3 Результатом выполнения стадии «Аванпроект» является техническое задание на создание ИС. В техническом задании должна быть документально оформлена политика ИБ с содержанием разделов:

- выбор критичных информационных ресурсов;
- анализ рисков для критичных информационных ресурсов;
- определение требований к средствам защиты;
- выбор основных решений по обеспечению режима ИБ;
- оценка остаточного риска;
- обеспечение бесперебойной работы организации.

Рекомендации по анализу рисков, определению требований к средствам ЗИ и оценке остаточного риска – по [2,3,4].

Требования к построению, содержанию и изложению ТЗ по СТ РК 1201.

6.3.4 Результатом выполнения стадии «Эскизный проект» является эскизный проект. Требования к выполнению документов по ГОСТ 2.119.

6.3.5 Результатом выполнения работ на стадии «Технический проект» является технический проект. Требования к выполнению документов по ГОСТ 2.120.

По результатам эскизного и технического проектирования ИС допускается, при необходимости, корректировать требования ТЗ в порядке, установленном для внесения изменений в утвержденное ТЗ по СТ РК 1201.

6.3.6 Результатом выполнения работ на стадии «Рабочая документация» является комплект конструкторской документации для изготовления и монтажа ИС, опытные образцы средств компонентов ИС прошедшие испытания в установленном порядке по программам и методикам согласованных с заказчиком, должностные инструкции персонала и пользователей ИС.

6.3.7 Результатом выполнения работ на стадии «Ввод в действие» является акт приемки ИС в промышленную эксплуатацию и сертификаты соответствия на аппаратное и программное обеспечение ИС, средства криптографической защиты информации и на информационную систему в целом, выданные соответствующими аккредитованными органами по подтверждению соответствия требованиям действующих нормативных документов по защите информации.

7 Общие требования к средствам ЗИ для обеспечения режима ИБ

Общие требования к средствам ЗИ для обеспечения режима ИБ включают:

- функциональные требования;
- требования к эффективности;
- технические требования;
- экономические требования (экономическое обоснование);
- требования к эксплуатационной документации.

7.1 Функциональные требования

Функциональные требования включают в себя следующие группы требований:

- грифы секретности обрабатываемой информации и категорию (класс защищенности) ИС;
- цели защиты информации;
- перечень защищаемой в ИС информации и требуемые нормы (уровни) эффективности ее защиты;
- возможные каналы утечки информации и способы несанкционированного доступа к ней, несанкционированные и непреднамеренные воздействия на информацию;

- задачи защиты информации в ИС.

7.1.1 Гриф секретности информации, категорию защиты (класс защищенности) ИС определяет заказчик на основании действующих нормативных документов [1].

7.1.2 Цель защиты информации – предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю, вследствие реализации угроз безопасности информации.

Цель защиты информации должна формулироваться для каждой стадии жизненного цикла ИС, иметь показатель эффективности достижения цели и требуемое его значение.

7.1.3 Перечень защищаемой в ИС информации и требуемые (нормы) уровни эффективности ее защиты

7.1.3.1 Конкретный перечень защищаемой информации в ИС должен определяться исходя из назначения ИС, целей ЗИ, состава и структуры ИС, а также составом и структурой средств ЗИ.

Перечень защищаемой информации определяется как для ИС в целом, так и для ее компонентов.

7.1.3.2 Требования по эффективности ЗИ должны включать:

- перечень реализуемых способов защиты информации;
- перечень показателей эффективности ЗИ;
- требуемые уровни эффективности ЗИ.

7.1.4 Выявление возможных каналов утечки информации, способов несанкционированного доступа к ней, несанкционированных и непреднамеренных воздействий на информацию должно осуществляться на основе анализа состава, структуры, алгоритмов функционирования и условий размещения ИС с использованием моделей угроз безопасности информации и факторов, воздействующих на защищаемую информацию. Классификация и номенклатура факторов, воздействующих на информацию - по СТ РК 1202.

7.1.5 Формулировка каждой задачи защиты информации должна включать:

- наименование конкретной угрозы безопасности для ИС и ее компонентов, которую необходимо предотвратить (устранить) при решении задачи;
- формулировку способа решения задачи;
- перечень функций, которые должны быть реализованы при решении конкретной задачи;
- требования к эффективности или гарантиям решения задачи;
- ограничения на ресурсы ИС, выделяемые на решение конкретной задачи.

7.1.5.1 Задачи ЗИ в ИС включают:

- предотвращение перехвата информации, передаваемой по каналам связи с помощью технических средств;
- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в ИС защищаемой информации;
- предотвращение несанкционированных или непреднамеренных воздействий, вызывающих разрушение, уничтожение, искажение защищаемой информации или сбои в работе средств ИС;
- выявление устройств перехвата информации, внедряемых в технические средства ИС;
- организацию разрешительной системы допуска пользователей ИС к работе с защищаемой информацией и ее носителями;
- уничтожение носителей информации;

- осуществление контроля функционирования систем и средств защиты информации в ИС.

7.2 Требования к показателям эффективности ЗИ

Перечень показателей эффективности ЗИ и требуемые уровни (нормы) эффективности ЗИ устанавливаются действующими нормативными документами.

7.3 Технические требования к средствам ЗИ

Технические требования к средствам ЗИ содержат требования к основным видам обеспечения ИС (техническому, программному), к зданиям (сооружениям, помещениям) или объектам, в которых ИС устанавливается, к размещению и монтажу аппаратуры и оборудования ИС, а также к средствам ЗИ и средствам контроля эффективности ЗИ.

7.3.1 Требования к средствам ЗИ содержат требования как к основным техническим средствам, применяемым по функциональному предназначению ИС, так и к вспомогательным техническим средствам, обеспечивающим функционирование основных технических средств.

7.3.1.1 Технические требования, предъявляемые к основным техническим средствам, содержат требования по ЗИ от утечки по ПЭМИН, от закладочных устройств, от внешних и внутренних факторов воздействующих на информацию, от несанкционированного доступа к информации и несанкционированных воздействий на нее.

Требования по ЗИ от утечки по ПЭМИН по СТ РК 34.013.

7.3.1.2 Технические средства ИС должны обеспечивать сохранность информации при отключении электропитания, при авариях, а также в условиях неблагоприятных природных явлений и стихийных бедствий.

7.3.1.3 Конструктивные требования, предъявляемые к техническим средствам ИС, должны формироваться с учетом требований по ЗИ и включаться в раздел «Конструктивные требования» ТЗ на разработку конкретного технического средства.

7.3.1.4 Требования к системе заземления и сети электропитания должны устанавливаться в соответствии с рекомендациями СТ РК 1200 и требованиями действующих нормативных документов.

7.3.1.5 Требования к монтажу сети телекоммуникаций (сети передачи данных) регламентируются действующими нормативными документами. Общие требования устанавливаются по СТ РК 1200.

7.3.1.6 Требования по ЗИ к программно-техническим средствам обеспечения ИБ включают группы требований:

- требования по разграничению доступа, управление доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- требования к учету, регистрации значительных событий для целей повседневного контроля и расследований;
- проверка и обеспечение целостности критически важных данных на всех стадиях их обработки;
- защита конфиденциальных данных от НСД, в том числе использование средств криптографической защиты;
- резервное копирование критически важных данных;
- восстановление работы ИС после отказов для систем с повышенными требованиями к доступности;
- защита от несанкционированных дополнений и изменений;

- требования к гарантиям, предусматривающие необходимость наличия в составе ИС технических и программных механизмов, позволяющих гарантировать выполнение требований к разграничению доступа и к учету.

7.3.1.7 Требования к средствам обработки информации в части устойчивости к внутренним факторам, воздействующим на информацию (отказы, сбои, ошибки) устанавливают совместно с требованиями по надежности и устойчивости функционирования конкретной ИС и ее компонентов по ГОСТ 21552.

Методы контроля, испытаний и приемки средств обработки информации устанавливают по ГОСТ 23773.

7.3.2 Требования к зданиям (сооружениям, помещениям) или объектам, в которых устанавливаются ИС, включают требования к контролируемой зоне, требования к ограждающим конструкциям здания (сооружения, помещения) или объекта, к технологии строительства, требования к средствам коммуникаций, требования к экранированию, звукоизоляции помещений и размещению оборудования.

Проектная конструкторско-технологическая документация, раскрывающая сущность замысла защиты, обоснование технических мероприятий ЗИ выпускается в ограниченном количестве экземпляров и на строительство не выдается. Открытое наименование раздела - «Дополнительные требования».

Размещение оборудования ИС отражается в техническом проекте в следующей документации:

- сводный план инженерных коммуникаций объекта (в масштабе) с указанием границы контролируемой зоны, местоположение объекта информатизации, трансформаторной подстанции, заземляющего устройства, трасс прокладки кабельных линий с указанием мест установки разделительных устройств и других элементов защиты;
- технологические поэтажные планировки сооружений (объекта) с указанием мест размещения технических средств обработки информации и режимных помещений;
- перечень устанавливаемых средств обработки информации, средств ЗИ и средств контроля с указанием наличия сертификата и мест их установки;
- перечень выделенных помещений;
- схемы систем активной защиты информации и размещения устройств акустической маскировки.

7.3.2.1 При необходимости реконструкции и расширения помещений (сооружений) объекта, в котором размещается ИС, требования по ЗИ предъявляются в соответствии со СНиП и другими действующими нормативными документами.

7.3.2.2 Общие рекомендации по размещению оборудования средств обработки информации - по СТ РК 1200. Размещение основных средств обработки информации должно производится с максимальным использованием экранирующих свойств здания (объекта), на нижних этажах, во внутренних помещениях на максимальном удалении от границ контролируемой зоны.

Компоненты и оборудование ИС следует размещать только в пределах контролируемой зоны, установленной для них в ЭД (для сертифицированных средств), предписаниями на эксплуатацию или результатами специсследований. Режимные помещения необходимо размещать на максимальных расстояниях от границ контролируемой зоны.

В помещениях, где установлено основное оборудование, запрещается прокладывать не относящиеся к нему кабели и провода, выходящие за пределы контролируемой зоны и не оборудованные средствами защиты.

Подключение кабелей к оконечным устройствам должно осуществляться через разъемы, обеспечивающие надежный электрический контакт между экранами кабелей и корпусами оконечных устройств.

Незадействованные разъемы, на которые выводятся цепи основных средств, должны закрываться экранирующими заглушками и опечатываться, а незадействованные отдельные контакты в разъемах – заземляться.

Коммутационные, распределительные и согласующие устройства основных средств обработки информации должны размещаться в металлических коробках или шкафах, крышки коробок и шкафов должны оборудоваться приспособлениями для опечатывания и сигнализацией на вскрытие.

Все свободные цепи кабелей должны быть замкнуты накоротко и заземлены в пределах контролируемой зоны.

Сеть передачи защищаемой информации должна быть выделенной, то есть не иметь подключений к другим сетям, в которых производится обработка открытой информации.

Оборудование ИС, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после пусконаладочных работ закрывается и опечатывается.

При размещении основных технических средств ИС в помещениях, предназначенных для ведения конфиденциальных переговоров, должны быть приняты меры по защите от утечки речевой информации по вибрационным и акустическим каналам.

Требования и методика контроля эффективности защиты помещений от утечки речевой информации по вибрационным и акустическим каналам – по СТ РК 1171.

7.3.2.3 Ограничения на аппаратные, программные, информационные, временные и другие ресурсы ИС, выделяемые на решение задач ЗИ, определяются с учетом имеющихся ресурсов ИС исходя из допустимого снижения эффективности функционирования ИС по основному предназначению.

7.4 Экономические требования по ЗИ

Экономические требования по ЗИ включают:

- допустимые затраты на создание ИС и системы ИБ ИС;
- допустимые затраты на эксплуатацию ИС и системы ИБ ИС.

7.4.1 Допустимые затраты на систему ИБ должны соотноситься с ценностью защищаемой информации и других информационных ресурсов, подвергающихся риску, а также с ущербом, который может быть нанесен организации из-за реализации угроз.

В результате анализа экономических показателей по критерию эффективность/стоимость уточняются допустимые остаточные риски и расходы по мероприятиям, связанным с применением конкретных вариантов ЗИ.

7.5 Требования к эксплуатационной документации по ЗИ

Общие требования к эксплуатационной документации по ГОСТ 2.601.

Дополнительно должна быть разработана следующая номенклатура документов, относящаяся к обеспечению режима ИБ.

7.5.1 Инструкция по управлению доступом пользователей к информационным ресурсам.

Инструкция предназначена для организации управления процессом предоставления прав доступа к информационным ресурсам и разрабатывается на все стадии жизненного цикла управления доступом пользователей - от начальной регистрации новых пользователей до удаления учетных данных пользователей, которые не нуждаются больше в доступе к информационным сервисам. Особое внимание должно быть уделено управлению процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.

7.5.2 Должностные инструкции персонала.

Инструкции устанавливают обязанности и ответственность персонала за обеспечение ИБ в соответствии с принятой политикой ИБ. В инструкциях отражается как общая ответственность за реализацию или поддержку политики ИБ, так и конкретные обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите.

Инструкции содержат разделы (в части касающейся категорий пользователей):

- работа с носителями информации;
- уничтожение носителей информации;
- работа с представителями сторонних организаций.

7.5.2.1 Раздел «Работа с носителями информации» организует работу со всеми носителями конфиденциальных данных: документами, отчетами, дискетами, жесткими дисками, компакт дисками, флэш-памятью и проч.

В разделе должно быть отражено:

- правила работы с носителями информации и их маркировка;
- регистрация получателей данных, имеющих соответствующие полномочия;
- обеспечение полноты входных данных;
- подтверждение получения переданных данных (по необходимости);
- категория лиц, которым предоставлен доступ к данным и их полномочия;
- маркировка всех копий данных для получателя, имеющего соответствующие полномочия;
- порядок обновления списков получателей с правом доступа к данным.

7.5.2.2 Раздел «Уничтожение носителей информации» определяет порядок уничтожения носителей информации и должен отражать:

- перечень носителей информации и их идентификацию;
- способ удаления (уничтожения) информации на носителях каждого типа (магнитные, бумажные), проверка гарантий удаления (уничтожения);
- порядок ведения журнала учета уничтожения (удаления) конфиденциальной информации.

7.5.3 Инструкция по администрированию ИС отражает обязанности администратора по надежной работе ИС и обеспечению режима ИБ. В инструкции должны быть описаны действия администратора ИС по выполнению каждого задания, в том числе:

- допустимые процедуры оперирования с файлами данных;
- требования к планированию выполнения заданий;
- действия по обработке ошибок и других исключительных ситуаций, которые могут возникать при выполнении зданий, в том числе ограничения на использование системных утилит;
- обращения за помощью в случае возникновения технических и других проблем, связанных с эксплуатацией ИС;
- порядок получения выходных данных и обеспечение их конфиденциальности, включая процедуры гарантированного удаления выходной информации в случае сбоя в работе ИС;
- процедуры перезапуска и восстановления работоспособности ИС после отказа.

В инструкции также должны быть разработаны разделы по процедуре перезапуска и остановки ИС, резервному копированию данных, техническому обслуживанию ИС, если эти вопросы не отражены в самостоятельных документах.

7.5.4 В комплект эксплуатационной документации должны входить:

- схема первичного электропитания основных и вспомогательных технических средств ЗИ;
- схема заземления основных и вспомогательных технических средств ЗИ;

- спецификация основных и вспомогательных средств ЗИ;
- спецификация программных средств, установленных в технических средствах ЗИ и в средствах контроля эффективности ЗИ;
- перечень оборудования, подлежащего периодическому контролю, объем и периодичность контрольных проверок;
- формуляр ИС;
- формуляр по ИБ.

7.6 Обеспечение режима ИБ при эксплуатации ИС

В процессе эксплуатации ИС должно быть организовано ограничение доступа к информации, блокирование физических каналов утечки и постоянный контроль реализации политики ИБ, основными направлениями которого являются:
- контроль работы пользователей;
- защита целостности данных и программ;
- управление доступом к приложениям;
- контроль внесения изменений.

7.6.1 Контроль работы пользователей

Контроль работы пользователей включает в себя:
- контроль сетевых подключений к конфиденциальным или критически важным приложениям и контроль полномочий доступа пользователей;
- управление доступом к рабочим местам путем идентификации и аутентификации пользователей, а также, при необходимости, терминала и местонахождение каждого зарегистрированного пользователя;
- ведение журнала учета попыток доступа (успешных и неудачных) к ИС;
- ограничение подключения пользователей в неурочное время;
- контроль процедур поддержания режима ИБ при выборе и использовании паролей;
- контроль оборудования, оставленного без присмотра и его защита от несанкционированного доступа;
- отслеживание времени простоя терминалов в зонах с повышенным риском нарушения ИБ;
- ограничение периода подключения терминала к ИС для пакетной передачи файлов;
- организация разрешительной системы для работы во внеурочное время;
- периодический анализ выходной информации ИС и, при необходимости, контроль удаления лишней информация.

7.6.2 Защита целостности данных и программ от вредоносного программного обеспечения

7.6.2.1 Защита от вирусов:
- организация должна проводить политику, требующую установки только лицензированного программного обеспечения;
- противовирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);
- необходимо проводить регулярную проверку целостности критически важных программ и данных, наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
- дискеты и другие сменные носители информации неизвестного происхождения должны проверяться на наличие вирусов до их использования;

- строго придерживаться установленных процедур по уведомлению о случаях поражения ИС компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

- планирование обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления, особенно для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

7.6.3 Управление доступом к сервисам

7.6.3.1 При использовании электронной почты рекомендуется:

- учитывать уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

- учитывать возможность неправильной адресации или направления сообщений не по назначению, а также надежность и доступность сервиса в целом.

7.6.3.2 Логический доступ к приложениям предоставляется только зарегистрированным пользователям. Приложения должны:

- контролировать доступ пользователей к данным и приложениям в соответствии с политикой управления доступом, принятой в организации;

- обеспечивать защиту от несанкционированного доступа к системным программам, которые способны обойти средства контроля и обеспечивают возможность НСД;

- не нарушать защиту других систем, с которыми они разделяют информационные ресурсы.

7.6.3.3 Для сведения риска повреждения программного обеспечения к минимуму, необходимо осуществлять жесткий контроль доступа к библиотекам исходных текстов программ. Рекомендуется придерживаться следующих правил:

- не хранить библиотеки исходных текстов программ в ИС;

- распечатки программ хранить в библиотеках исходных текстов;

- ограничивать доступ к библиотекам исходных текстов программ;

- обновление библиотек исходных текстов программ и выдача текстов программ программистам должны производиться только назначенным ответственным сотрудником после получения разрешения в установленной форме на доступ к приложению;

- необходимо фиксировать все случаи доступа к библиотекам исходных текстов программ в контрольном журнале;

- устаревшие версии исходных текстов программ следует архивировать с указанием даты окончания их использования вместе со всем вспомогательным программным обеспечением и информацией об организации выполнения заданий для этой версии программного обеспечения;

- сопровождение и копирование библиотек исходных текстов программ необходимо осуществлять в соответствии с процедурами управления процессом внесения изменений.

Все чрезвычайные ситуации и события, связанные с нарушением режима ИБ, необходимо регистрировать в журнале. Журнал следует хранить в течение заданного промежутка времени. Кроме неудавшихся попыток входа в систему, целесообразно также регистрировать случаи успешного доступа. Контрольный журнал должен включать:

- идентификаторы пользователей;

- дата и время входа и выхода из системы;

- идентификатор или местонахождение терминала (по возможности);

- неудачные попытки доступа в ИС;

- попытки несанкционированного использования восстановленных пользовательских идентификаторов;

- использование ресурсов с привилегированным доступом;
- отдельные действия, потенциально опасные с точки зрения нарушения режима ИБ;
- использование конфиденциальных ресурсов.

7.6.4 Внесение изменений

Внесение изменений в ИС и ее компоненты должно производиться в соответствии с утвержденными процедурами, после обязательной оценки влияния вносимых изменений на режим ИБ.

В необходимых случаях должны быть проведены типовые испытания с целью проверки соответствия характеристик и параметров ИС установленным требованиям после внесения изменений.

Необходимость проведения типовых испытаний определяет разработчик по согласованию с органами надзора (контроля).

Правила доведения внесенных изменений до сведения лиц, которых они затрагивают, должны определяться в инструкциях персоналу в части касающейся непосредственных обязанностей.

Приложение
(справочное)

Библиография

[1] Сборник нормативных правовых актов по защите государственных секретов. – Астана; Агентство по защите государственных секретов, 2002.

[2] Рекомендации ИСО/МЭК 15408-1:2005 Технологии информационные. Методы защиты. Критерии оценки защиты информационных технологий. Часть 1. Введение и общая модель.

[3] Рекомендации ИСО/МЭК 15408-2:2005 Технологии информационные. Методы защиты. Критерии для оценки защиты информационных технологий. Часть 2. Эксплуатационные требования безопасности.

[4] Рекомендации ИСО/МЭК 15408-3:2005 Технологии информационные Методы защиты. Критерии для оценки защиты информационных технологий. Часть 3. Требования к обеспечению защиты.

УДК **МКС 35.240**

Ключевые слова: информационная система, информационная безопасность, средства защиты информации, режим информационной безопасности, стадии и этапы разработки

Для заметок

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Есіл өзеннің жағалауы, № 35 көше, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074