Об организации допуска и доступа к информации различных категорий конфиденциальности в автоматизированных системах класса «3» на примере АРМ «Гражданский Щит»

Прималенный Александр Алексеевич - *ООО «Крымское аэрокосмическое агентство», научный руководитель программы АРМ «Гражданский Щит», кандидат географических наук*

Егоров Федор Иванович - *начальник Управления Госспецсвязи Украины в г. Севастополе, полковник Госспецсвязи Украины*

Одним из переходных противоречий развития культуры правового демократического государства с рыночным (конкурентным) хозяйственным укладом является сопряженное действие права Общества на информацию об аспектах жизнедеятельности территориальной общины при одновременном праве граждан на тайну личной жизни. Как следствие, если порядок обработки каких-то данных не оговорен законодательно (или по решению суда), лицам, принимающим решения, приходится сталкиваться с персональной ответственностью «назначения приоритета»:

- права Общества в лице отдельных групп населения, вынужденных организовывать производство и быт в условиях хозрасчета для нужд собственного функционирования и развития, получать информацию о конкретных фактах, например, природопользования, домовладения, др.,

  либо

- права Гражданина - каждого члена Общества - на минимизацию доступа к информации о нем для исключения, как минимум, недобросовестной конкуренции и суждений.

С ростом качества аппаратно-программных средств и совершенствования информационных технологий, проблема защиты информации об отдельном гражданине с одновременным ее законодательным «дозированием» для сведения посторонних (в каждом конкретном случае) гражданину физических, юридических лиц и учреждений становится все более сложной.

Причиной тому является:

- распад единых государственных и коммунальных систем, обрабатывавших данные о гражданах (жилье, услуги коммунальных предприятий, медицина);
- разобщенность систем отчетности административно неподчиненных субъектов – работодателей и собственников жилищных объектов, предприятий, земельных наделов, инженерной инфраструктуры и средств производства;
- несопоставимый по эффективности аппаратно-технический и программно-технологический уровень обработки данных над рутинной архивацией данных, что приводит к многократному превышению возможностей сбора, хранения, тиражирования и распространения информации;
- посещение глобальной информационной сети с технических средств, хранящих конфиденциальную информацию и другие факторы.

Таким образом, в основе противоречия оказываются единство и противоположность:

- необходимости расширения информационного поля об Обществе, Бизнесе и Власти в интересах контроля отдельными личностями и их объединениями формирования и выполнения Генеральных планов городов, что невозможно без сбора информации о характере использования каждого земельного участка в пределах этих интересов (но не более территории государства);
- необходимости минимизации возможности несанкционированного сбора информации о жизнедеятельности одних граждан со стороны других граждан, в том числе - через государство.

Сложность решения данного парадокса **«о других все – обо мне ничего»** заключается:

- в неконкретности законодательной базы о гражданской тайне (и коммерческой в том числе), в отличие от тайны государственной, охрана которой решена достаточно корректно через объявление перечня сведений, ее составляющих, и уровне их конфиденциальности, определяющей порядок допуска к ознакомлению с ними;
- в бесперспективности гражданской цензуры в правовом, демократическом государстве: рецепт охраны гражданской тайны через режимные отделы вряд ли применим в частной жизни граждан и их объединений (в том числе - корпоративных на коммерческой основе);
- в беспечности частных пользователей при обмене «дружественной информацией» через глобальные сети с применением аппаратных средств, обрабатывающих «закрытую» информацию без ее защиты от несанкционированного «недружественного» доступа третьих лиц.

Следует отметить, что идеологическая сложность внедрения **государственных стандартов** по ограничению **допуска** к информации о личной жизни и коммерческой деятельности граждан и их объединений может достаточно успешно компенсироваться **нормативно-отраслевой практикой** защиты информации «как таковой по ГОСТ», позволяющей без создания режимного отдела:

- организовать защиту частных баз данных в персональных компьютерах (и локальных сетях передачи данных) от внешних атак на «целостность» и «доступность» личной информации из глобальной сети и/или взаимодействующих при обработке информации смежных локальных сетей;
- организовать раздельный **доступ** к частной информации через создание конфиденциальных областей баз данных (доменов), чем отделить их от обработки «открытой» информации;
- присвоить «закрытым» доменам частной информации 4-ю категорию конфиденциальности с организацией **допуска** «Для служебного пользования» и соответствующего наблюдения.

Во-первых, эти меры реально защищают сферу применения частной информации при использовании технических средств ее обработки.

Во-вторых, нарушение третьими лицами реализованных мер самозащиты КАК ПРЕЦЕДЕНТ является доказательной базой для граждан (организаций) при реализации конституционного права на судебную защиту от несанкционированного доступа и/или сбора информации: выявить и доказать нарушение границ частной (личной и/или) коммерческой тайны каким-либо иным способом достаточно сложно по причине законодательной неконкретности этих понятий.

Меры самозащиты реализуются путем привязки такого проекта к нормативной базе по технической защите информации (НД ТЗИ) в автоматизированных системах (АС):

1) АС класса «1» в виде одномашинного однопользовательского (по функциональным возможностям) комплекса, обрабатывающего информацию одной или нескольких категорий конфиденциальности в защищенной среде (контролируемой зоне); пример – автономная персональная ЭВМ, доступ к которой контролируется организационными мерами, обеспечивая обработку информации разных категорий конфиденциальности разных пользователей, но работающих не одновременно (последовательно):
   - закреплению очередности и/или времени пользования (доступа);
   - созданию пользовательских доменов с разделением их внутри на «открытые» и «закрытые» базы данных (базовые домены);
   - распознаванию пользователей посредством идентификации «свой – чужой» через систему паролей и аутентификации «кто конкретно» через считывание уникальных особенностей пользователей (при наличии такой необходимости на усмотрение владельца комплекса);

2) АС класса «2» в виде локализованного многомашинного многопользовательского (по функциональным возможностям) комплекса, на котором обрабатывается информация разных категорий конфиденциальности; существенное отличие от предыдущего класса – наличие пользователей с разными полномочиями по доступу к информации и/или технических средств, которые могут одновременно осуществлять обработку информации разных категорий конфиденциальности; пример - локальная вычислительная система (ЛВС), доступ к которой по пользовательским и базовым доменам в центральном сервере ЛВС должен быть организован идентично АС класса «1».

Из краткого описания особенностей доступа в автоматизированных системах класса «1» и класса «2» следует, что подобные системы являются типовыми (что удобно) для ситуаций, где имеется контролируемая собственником АС (за посторонними лицами) зона (снаружи) и наблюдается (изнутри):

- количество пользователей и признаки их распознавания;
- уровень доступа к пользовательским и базовым доменам информации каждого пользователя;
- очередность и время доступа пользователей.

Но принципиальной составляющей сущности данной АС является знание ее собственником обрабатываемой (по его собственной инициативе) частной информации о личной жизни.

Данный принцип существенного знания наблюдается и в рамках отраслевых информационных технологий, где граждане могут (в том числе через судебные решения) контролировать уровень обработки информации (получение, использование, распространение и хранение) О СЕБЕ, поскольку они представляют ее в контролирующие ведомства САМИ и ДОЗИРОВАННО.

Иначе складывается ситуация с обработкой информации о гражданах в информационной деятельности местного самоуправления, особенно при формировании и выполнении Генерального плана населенного пункта:

- разрабатывать «де юре» его необходимо с учетом частных, общественных и государственных интересов в рамках административных границ жизнедеятельности территориальной громады;
- разрабатывать «де факто» его приходится в отсутствие подавляющего большинства планов развития домашних хозяйств (личных интересов) и их жилищных, корпоративных и общественных объединений; причин тому несколько, но все они являются следствием отсутствия теории собственности в государстве и самой собственности (в первую очередь на средства производства) у большинства граждан при желании у них эту собственность, в первую очередь, земельные наделы, получить.

Как следствие, в рамках данного парадокса органы местного самоуправления могут представить информацию для необходимого контроля Обществом в виде достаточной информации о членах Общества (что неудобно) с исключением при этом возможности недружественного ее использования.

При этом:

1. Достаточность информации местного самоуправления для Общества не должна ограничиваться ее режимностью за счет ограничения пределов знания, но должна быть разграничена:

а) с допуском «открытой» информации и доступом (в растровом формате) через защищенную часть городской глобальной сети (ЗГГС) с распознаванием места запроса: для гостей и жителей (членов территориальной громады) города - об объектах недвижимости города с раскрытием их отраслевых функций (жилые дома, гостиницы, АЗС, кинотеатры, рестораны и т.п.), адреса, маршрута проезда и т.д.;

б) с допуском «для служебного пользования» и доступом (в растровом формате) через ЗГГС с распознаванием места запроса и пользователя - для жителей (членов территориальной громады) о характере (явлении) собственности на средства производства:

- форма - недвижимость, земельные участки, инфраструктура;
- содержание - государственная, коммунальная, корпоративная, частная, совместная и т.п.;
- сущность - владение, пользование, распоряжение, -

что позволит создание необходимого и достаточного количества сценариев качества производственных отношений в интересах интеллектуальной поддержки принятия решения органами местного самоуправления по оптимизации размещения производительных сил и «прозрачности» этих решений.

в) с допуском «для служебного пользования» и доступом (в векторном формате) через глобальную сеть с распознаванием места запроса и пользователя - для жителей (членов территориальной громады) о материальном и финансовом состоянии их собственности и составе сособственников.

2. Для органов власти потребность контроля и управления сопряженным развитием и функционированием города потребуют, кроме уровня исследования ситуации в интересах граждан и их объединений, также анализ, прогноз и оценку последствий от принятия решений, в том числе в интересах формирования и выполнения «прозрачного для Общества» Генерального плана.

В рамках НД ТЗИ обработка информации с применением глобальных сетей реализуется на базе АС класса «3» как распределенного многомашинного многопользовательского комплекса, на котором (одновременно) обрабатывается информация разных категорий конфиденциальности с необходимостью передачи информации через незащищенную среду и наличии узлов, реализующих различную политику безопасности, как это представлено на примере АРМ «Гражданский Щит» (рис. 1):

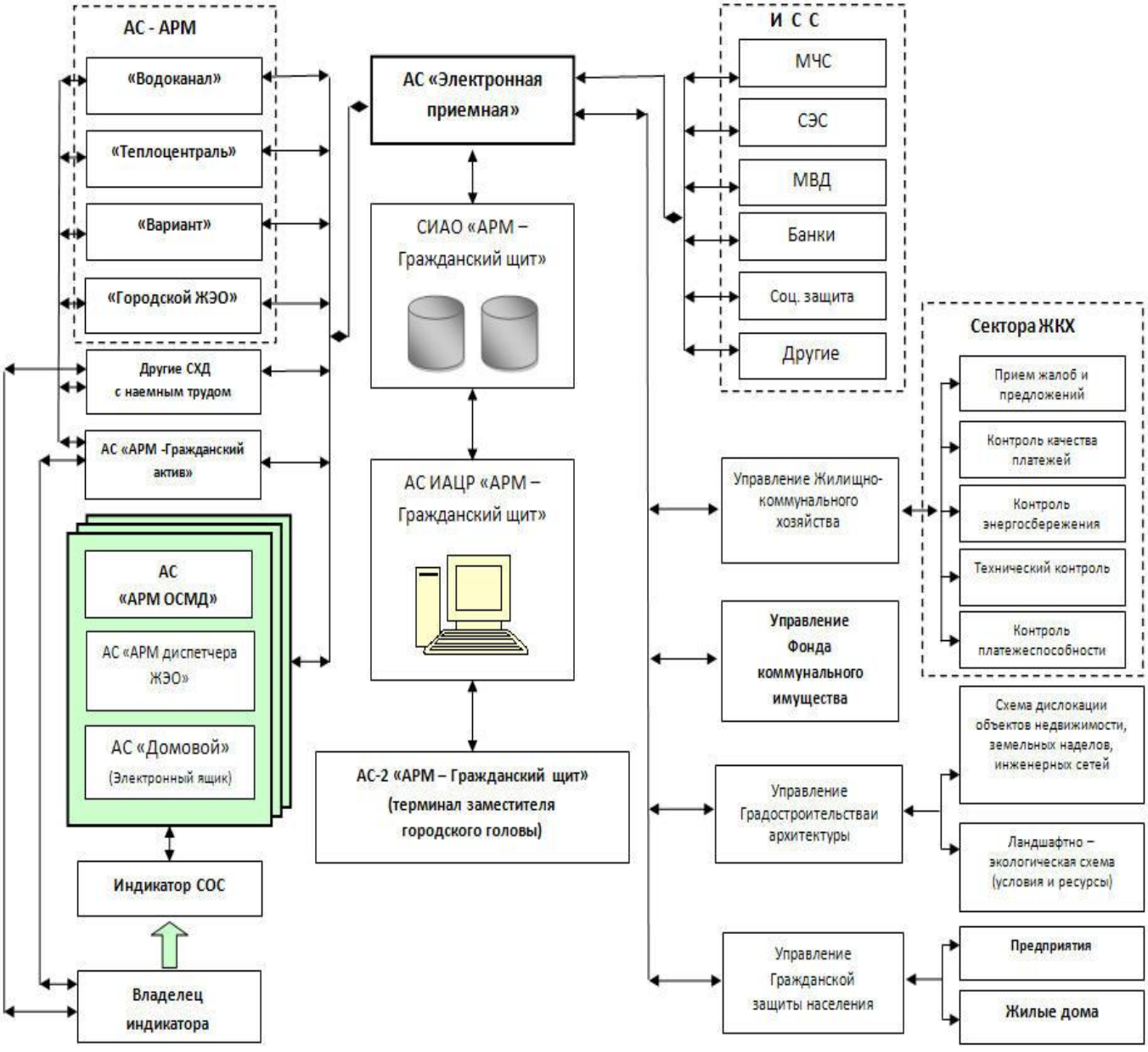

Рис. 1. Контрагенты автоматизированной системы класса «3» на примере АРМ «Гражданский Щит»

При этом обработку информации о гражданах следует производить в рамках статистического метода горизонтального и вертикального учета данных, что исключит несанкционированный доступ к сводной информации о личности гражданина, и одновременно обеспечит создание искомой системы обезличенных реестров различных конфигураций и различной категории безопасности на базе каждой из позиций сводной информации о личности.

Реализация заданных требований по построению АС класса «3» на базе ЗГГС в условиях незащищенной среды передачи информации различных пользовательских конфигураций и различной категории безопасности при концептуальном исключении допуска к частной информации формализуется в следующей последовательности:

1. Производится системное описание искомой информационной базы задачи.

2. Под информационную базу задачи определяются «замкнутые» целевые информационные системы и формируется информационная концепция проектируемой АС класса «3».

3. На базе концепции формируется перечень «подчиненных» целевых АС (АС-1, АС-2, АС с выходом в INTERNET) как целостной АС класса «3».

4. Формулируется требования к выделенным помещениям под целевые АС и способам передаче данных между целевыми АС в составе АС класса «3».

5. Разрабатывается перечень выполнения обязательных мероприятий, предусмотренных действующей нормативной базой по созданию целевых АС с комплексной системой защиты информации (КСЗИ) в АС (далее – АС с КСЗИ).

6. Определяются перечень обязательных мероприятий и разрабатываемых документов по этапам разработки (табл. 1):

Таблица 1

№	**Перечень обязательных мероприятий и разрабатываемых документов**
	Предпроектная подготовка
1.1	Общее знакомство с собственником предполагаемой АС и заключение договоров
1.2	Разработка документов:
•	Приказ о назначении ответственных лиц за защиту информации в создаваемой АС
•	Положение о службе защиты информации в АС.
•	Утверждение состава компетентной комиссии для проведения обследований, категорирования, принятия и оценки результатов выполнения работ в процессе создания АС с КСЗИ
•	Разработка проекта перечня объектов, в которых циркулирует конфиденциальная информация (КИ) с использованием ВС и АС, которые действуют и/или проектируются, и выделенных для них помещений (ВП)
•	Разработка проекта перечня сведений с ограниченным доступом (КИ), обрабатываемой в АС с КСЗИ
1.3	Сбор информации об ОИД (на основе «Опросного листа»), отражающей все факторы (в рамках заявленного уровня защиты) влияющие на безопасность информации указанной в разработанном проекта перечня.
1.4	Разработка структуры ИД на ОИД с локализацией информационных потоков
1.5	Разработка структуры взаимодействия подразделений ОИД с выявлением целевых АС как структуры АРМ класса «3»
1.6	Утверждение документов
•	Утверждение перечня сведений с ограниченным доступом (КИ), обрабатываемой в целевых АС
•	Утверждение перечня объектов, в которых циркулирует КИ с использованием ВС и АС, которые действуют и/или проектируются, и выделенных для них помещений (ВП)

1	***Этап 1. Создание целевых АС в составе АРМ класса «3»***
1.1	Разработка и Согласование в установленном порядке - Пояснительной записки «Структура АРМ класса «3» на базе перечня и схемы территориального размещения ОИД АС. - ТЗ на создание целевых АС с учетом требованиями по ТЗИ
1.2	Разработка технорабочих проектов на создание АС в соответствии с требованиями ТЗ (при создании новых АС)
1.3	Подготовка комплекта эксплуатационных документов на имеющиеся ВС с целью создания необходимого пакета документов на АС в рамках дальнейшего создания КСЗИ в АС и в соответствии с требованиями ТЗ на создание целевых АС (при создании КСЗИ в АС не имеющей проектной документации)
1.4	Реализация технорабочих проектов (требований ТЗ) на создание АС
2	***Этап 2. Разработка системы защиты информации***
2.1	Разработка и утверждение организационных документов
2.2	Разработка проекта плана план защиты информации
2.3	Обследование ОИД АС на соответствие требованиям технических проектов АС. Составление актов по результатам обследования
2.4	Категорирование элементов АС (ВС, информации, ВП):
2.5	Разработка и согласование в установленном порядке моделей угроз для каждого ОИД АС
2.6	Разработка и согласование в установленном порядке технических заданий на создание КСЗИ в АС различных классов
2.7	Корректировка и утверждение плана план защиты информации
2.8	Разработка плана технической защиты информации в АС.
2.9	Разработка положений и должностных инструкций служб и лиц связанных с обработкой защищаемой информацией в АС для обеспечения защиты информации.
2.10	Разработка и согласование в установленном порядке технорабочего проекта АС и КСЗИ в АС.
2.11	Разработка рабочей документации на АС и КСЗИ в АС
3	***Этап 3. Реализация проекта защиты информации.***
3.1	Внедрение организационных, первичных технических мер защиты информации.
•	Применение специальных инженерно-технические сооружений, средств (систем)
3.2	Реализация основных технических мер защиты.
•	Размещение, монтаж и наладка вспомогательных технических средств и систем АС
•	Размещение, монтаж и наладка основных технических средств АС
•	Установка средств ТЗИ.
•	Инсталляция, настройка и тестирование аппаратных и/или программных средств защиты информации.
4	***Этап 4. Контроль функционирования и управление системой защиты информации. Аттестация АС.***
4.1	Аттестация АС и КСЗИ в АС.
4.2	Подготовка (обучение) персонала и пользователей к эксплуатации АС.
4.3	Предварительные испытания АС и КСЗИ на основе ПМА и ПМпИ
4.3.2	Устранение замечание выявленных на предварительных испытаниях
4.3	Испытания АС и КСЗИ на основе ПМА и ПМИ
3.5	Выполнение инструментального контроля объекта ТЗИ: спецобследований на закладные устройства и специсследований на уровни ПЭМИН технических средств АС.(при необходимости)
4.4	Опытная эксплуатация АС

РАЗРАБОТКУ технических проектов по созданию целевых АС-1 с КСЗИ на базе утвержденных технических заданий желательно вести в следующем порядке, отличающего от структуры АС-2 с КСЗИ наличием системы передачи данных (табл. 2):

Таблица 2

РАЗДЕЛ I. Сведения об АС для проектируемой КСЗИ	
1	**Общие положения**
1.1	Назначение проекта
1.2	Наименование проектируемой КСЗИ, назначение и область применения
1.3	Наименование документов, на основании которых разрабатывается проект
1.4	Перечень организаций, которые принимают участие в создании КСЗИ
1.5	Сроки выполнения и очередность создания КСЗИ
1.6	Соответствие проектных решений действующим нормам и правилам безопасности
1.7	Сведения об использовании НД, НДР, передового опыта
2	**Описание АС-1 как конечного продукта**
2.1	Общая характеристика АС-1
2.2	Цель и назначения АС-1
2.3	Цель и назначения КСЗИ в составе АС-1
2.4	Структура (элементы и компоненты) АС-1
2.5	Характеристика вычислительной системы
2.6	Характеристика персонала АС-1
2.7	Характеристика физической среды
2.8	Характеристика обрабатываемой информации как продукции АС-1
2.9	Характеристика технологий обработки информации как процессов АС-1
2.10	Характеристика условий функционирования
2.11	Характеристика ОИД с использованием АС-1
РАЗДЕЛ II. Проектные решения по организации защиты информации в АС-1	
3	**Проектные решения по достижению необходимых характеристик АС-1**
3.1	Общие положения
3.2	Решение по программному обеспечению АС-1
3.3	Решение по комплексу основных технических средств АС-1
3.4	Решение по комплексу вспомогательных технических средств и систем АС-1
3.5	Решение по информации, которая циркулирует на ОИД с использованием АС-1
3.6	Решение по взаимосвязи АС-1 с сопредельными системами
3.7	Решение по обрабатываемой информации как продукции АС-1
3.8	Решение по технологии обработки информации в АС-1
3.9	Решение по персоналу АС-1
3.10	Решение по соблюдению действующих норм и правил безопасности
3.11	Решение по составу документации АС-1

4	**Проектные решения по достижению необходимых характеристик ОИД АС-1**
4.1	Общие положения по инженерно-техническим мероприятиям
4.2	Решение по инженерно-техническим сооружениям
4.3	Решение по системам жизнеобеспечения
4.4	Решение по заземлению
4.5	Решение по инженерно-техническому обеспечению условий функционирования
4.6	Решение по соблюдению действующих норм и правил безопасности
4.7	Решение по составу документации на ВП как ОИД АС-1
5	**Проектные решения по достижению необходимых характеристик КСЗИ в составе АС-1**
5.1	Общие положения о КСЗИ в составе АС-1
5.2	Решение по концепции защиты информации:
5.2.1	Решение по политике безопасности услуг
5.2.2	Решение по ограничения видов обработки информации
5.2.3	Решение по ограничению применения программного обеспечения
5.2.4	Решение по ограничению доступа персонала
5.2.5	Решение по ограничению доступа посетителей
5.2.6	Решение по контролируемой зоне и территории
5.3	Решение по модели защиты информации
5.3.1	Решение по защите информации от НСД
5.3.2	Решение по защите информации от утечки по техническим каналам
5.3.3	Решение по защите информации от электромагнитного влияния
5.4	Решение по средствам защиты информации
5.4.1	Решение по архитектуре и интерфейса средств ТЗІ
5.4.2	Решение по оснащению АС-1 средствами ТЗІ
5.4.3	Решение по тестированию КСЗИ в АС-1
5.5	Решение по функциональным услугам КСЗ от НСД
5.6	Решение по соблюдения действующих норм и правил безопасности
5.7	Решение по составу документации КСЗИ в составе АС-1
6	Сведения о соответствии технического задания на КСЗИ и проекта
7	Сведения о закупке технических и программных средств
7.1	Решение по закупке основных и вспомогательных технических средств и систем
7.2	Решение по закупке программного обеспечения
7.3	Решение по закупки средств ТЗИ

РАЗДЕЛ III. Реализация проекта КСЗИ в составе АС-1	
8	Организационные мероприятия по защите информации
9	Первичные технические мероприятия по защите информации
10	Основные технические мероприятия по защите информации
11	Пусконаладочные работы
12	Приемка, определение полноты и качества работ
13	Опытная эксплуатация АС-1 и КСЗИ в составе АС-1
14	Государственная экспертиза КСЗИ в составе АС-1
15	Введение в эксплуатацию АС-1
РАЗДЕЛ IV. Сервисное обслуживание в период эксплуатации	
16	Сервисное обслуживание ОТС и ВТСС
17	Сервисное обслуживание КСЗИ

Приложение 1.	Перечень использованных нормативно-технических документов
Приложение 2.	Общий перечень работ при создании АС-1 и КСЗИ в составе АС-1
Приложение 3.	Номенклатура документации в составе проекта КСЗИ в АС-1
Приложение 4.	Короткое описание КЗЗ от НСД «Гриф»
Приложение 5.	Сведенная спецификация оборудования и программного обеспечения АС-1
Приложение 6.	Генеральный план ВП, общий вид
Приложение 7.	Схема размещения, которое рекомендуется, ОТС АС-1
Приложение 8.	Схема размещения, которое рекомендуется, ВТСС АС-1
Приложение 9.	Схема размещения, которое рекомендуется, средств ТЗИ

Применяемые сокращения:

ВТСС	-	вспомогательные технические средства и системы
КИ	-	конфиденциальная информация, не являющаяся собственностью государства
КСЗ	-	комплекс средств защиты
НСД	-	несанкционированный доступ
ВС	-	вычислительная система
ОТС	-	основные технические средства
ПМА	-	программа и методика аттестации
ПМпИ	-	программа и методика предварительных испытаний
ПМИ	-	программа и методика испытаний
ПО	-	программное обеспечение
ТЗ	-	техническое задание
ТЗИ	-	техническая защита информации

Литература:

- Закон Украины «Про Національну програму інформатизації» от 04.021998 г. № 74 / 98-ВР.
- «Положення про формування та виконання Національної програми інформатизації», утвержденное постановлением Кабинета Министров Украины от 31 июня 1998 года № 1352.
- Закон Украины « Про місцеве самоврядування в Україні ».
- ДСТУ 3396.0-96-ДСТУ 3396.2-97 «Захист інформації. ТЕХНИЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»;
- Другие требования нормативно-правовой базы Украины по технической защите информации.