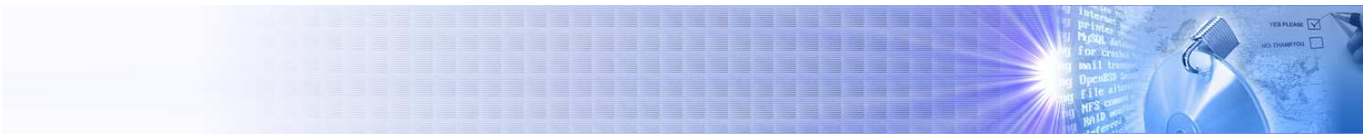
К С З И

(комплексные системы защиты информации)

ОГЛАВЛЕНИЕ



Определение КСЗИ

Комплексные системы защиты информации (КСЗИ) представляют собой совокупность мероприятий, которые можно поделить на две основные категории:

- организационные;
- инженерно-технические.

Все эти мероприятия направлены на обеспечение защиты критичной информации от утечки, нарушения целосности и несанкционированного доступа.

При построении любой КСЗИ, обязательной и важнейшей составляющей являются организационные мероприятия. Инженерно-технические – выполняются по необходимости.

Организационные мероприятия

Обеспечивают управление, документальное закрепление положений по информационной безопасности и определяют ответственность за нарушение установленного режима информационной безопасности.

Организационные мероприятия включают в себя следующие концепции информационной безопасности:

- Составление должностных инструкций для пользователей и обслуживающего персонала;
- Создание правил администрирования системы, учета, хранения, размножения, уничтожения носителей информации, идентификации пользователей;
- Разработка порядка действия в случае выявления попыток несанкционированного доступа к информационной системе или выхода из строя средств защиты информации.
- Обучение пользователей правилам информационной безопасности.

Инженерно-технические мероприятия

Совокупность специальных технических средств[1] обеспечивающих установленный в организации режим безопасности и защиты информации. Выбор инженерно-технических мероприятий зависит от необходимого уровня защищенности информации.

Инженерно-технические мероприятия, проводимые для защиты информационной инфраструктуры организации, могут включать использование следующих средств:

- защищенные подключения;
- межсетевые экраны;
- разграничение потоков информации между сегментами сети;

[1]Согласно Закона Украины «О защите информации в информационно-телекоммуникационных системах» для создания комплексной системы защиты информации, являющейся собственностью государства, или информации с ограниченным доступом, требование к защите которой установлена законом, используются средства защиты информации, которые имеют сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере технической и/или криптографической защиты информации.

- средства шифрования и защиты от несанкционированного доступа.

В случае необходимости, в рамках проведения инженерно-технических мероприятий, в помещениях может осуществляться установка систем: охранно-пожарной сигнализации, контроля и управления доступом.

Отдельные помещения могут быть оборудованы средствами защиты от акустической утечки информации, от побочных электромагнитных излучений и наводок (ПЭМИН) и т.н. «закладок»[2].

Субъекты КСЗИ

В процесс создания КСЗИ вовлекаются следующие стороны:

Заказчик: организация, для которой осуществляется построение КСЗИ;

Исполнитель: организация, осуществляющая мероприятия по построению КСЗИ;

Организатор экспертизы: организация, осуществляющая государственную экспертизу КСЗИ;

Подрядчик: организация, привлекаемая в случае необходимости Заказчиком или Исполнителем для выполнения некоторых работ по созданию КСЗИ.

Объекты защиты КСЗИ

Объектами защиты КСЗИ является информация в любом ее виде и форме представления.

Материальными носителями информации являются сигналы. По своей физической природе информационные сигналы бывают следующих видов:

- электрические;
- электромагнитные;
- акустические;
- комбинированные.

Сигналы могут быть представлены в форме электромагнитных, механических и других видов колебаний, при этом информация, подлежащая защите, содержится в их изменяющихся параметрах.

В зависимости от природы, информационные сигналы распространяются в определенных физических средах. Среды бывают газовыми, жидкостными и твердыми. Например: воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и другие.

В зависимости от вида и формы представления информационных сигналов, которые циркулируют в информационно-телекоммуникационной системе (ИТС), в том числе и в автоматизированных системах (АС), при построении КСЗИ могут использоваться различные средства защиты.

Компания "АТМНИС" специализируется на предоставлении услуг в сфере создания КСЗИ АС всех классов [3]:

- одномашинных пользовательских комплексов (АС класса 1);
- локализованных многомашинных многопользовательских комплексов (АС класса 2);
- распределенных многомашинных многопользовательских комплексов (АС класса 3).

[2] Внедренные специальные электронные устройства негласного съема информации

[3] Согласно НД ТЗИ 2.5-005-99 «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа» – автоматизированная система (АС) представляет собой организационно-техническую систему, которая объединяет вычислительную систему, физическую среду, персонал и обрабатываемую информацию.

Необходимость построения КСЗИ [4]

Согласно требований закона[5], вся информация, являющаяся собственностью государства, или информация с ограниченным доступом[6], должна обрабатываться в системе с применением комплексной системы защиты информации с подтвержденным соответствием. Подтверждение соответствия осуществляется по результатам государственной экспертизы в порядке, опередленном законодательством.

Согласно закона Украины «О защите информации в информационно-телекоммуникационных системах»:

- информация, являющаяся собственностью государства или информация с ограниченным доступом, должна быть защищена путем построения КСЗИ с получением «Аттестата соответствия», который выдается ГСССЗИУ;
- прочая информация может быть защищена с помощью КСЗИ по желанию владельца.

Необходимость построения КСЗИ определяется требованием нормативных документов или желанием владельца информационных ресурсов.

Этапы построения КСЗИ

Построение КСЗИ состоит из следующих этапов:

1. Подготовка организационно-распорядительной документации.
2. Обследование информационной инфраструктуры Заказчика.
3. Разработка «Плана защиты информации».
4. Разработка «Технического задания на создание КСЗИ».
5. Разработка «Технического проекта на создание КСЗИ».
6. Приведение информационной инфраструктуры Заказчика в соответствие с «Техническим проектом на создание КСЗИ».
7. Разработка «Эксплуатационной документации на КСЗИ».
8. Внедрение КСЗИ.
9. Испытание КСЗИ.
10. Проведение государственной экспертизы КСЗИ и получение «Аттестата соответствия».
11. Поддержка и обслуживание КСЗИ.

В этапах № 1–11 принимают участие Исполнитель и Заказчик. На этапе № 10 к работе подключается организатор экспертизы. Для этапов № 6 и 8 могут привлекаться Подрядчики.

После принятия Заказчиком решения о создании КСЗИ между Заказчиком и Исполнителем подписывается договор о создании КСЗИ, в котором должны быть описаны порядок и сроки выполнения[7], а также стоимость работ.

---

[4] Закон Украины «О защите информации в информационно-телекоммуникационных системах» от 31.05.2005 № 2594 - IV. Статья 8 *«Условия обработки информации в системе».*

[5] Постановление Кабинета Министров от 29.03.2006г. № 373

[6] Например: конфиденциальная информация.

[7] Этапы работ, которые выполняются во время создания КСЗИ, их содержание, результаты и сроки выполнения определяются ТЗ на создание КСЗИ на основании приказа ДСТСЗИ СБУ № 125 от 08.11.2005 "Об утверждении Порядка проведения работ по созданию комплексной системы защиты информации в информационно-телекоммуникационной системе".

1. Подготовка организационно-распорядительной документации

На этом этапе специалисты Исполнителя проводят анализ организационно-распорядительных документов Заказчика и нормативно-правовых документов в области защиты информации, влияющих на деятельность Заказчика.

К организационно-распорядительным документам обычно относятся:

- организационная структура;
- штатное расписание;
- положение об отделах;
- должностные инструкции сотрудников, связанных с эксплуатацией ИТС;
- документы, регламентирующие доступ к ИТС;
- прочее.

К нормативно-правовым документам в области защиты информации относятся:

- законы Украины;
- постановления Кабинета Министров Украины;
- приказы ГСССЗИУ, устанавливающие правила работы с информацией.

По результатам выполнения этого этапа Исполнитель готовит проекты документов, которые определяют организационную составляющую КСЗИ (проект приказа о созданиии КСЗИ, проект положения о службе защиты информации, проекты должностных инструкций, процедур и др.), которые утверждаются Заказчиком.

2. Обследование информационной инфраструктуры Заказчика

На этом этапе специалисты Исполнителя проводят обследование ИТС Заказчика.

Анализируется архитектура системы, ее топология и составляющие элементы. Определяются типы пользователей системы, типизируется информация, обрабатываемая в ИТС.

По результатам выполнения этапа Исполнитель разрабатывает следующие документы:

- акт обследования ИТС (содержит описание, принципы построения и архитектуру ИТС);
- перечень объектов ИТС, которые подлежат защите, утверждаемые Заказчиком.

3. Разработка плана «Защиты информации»

По результатам выполнения второго этапа, а именно основываясь на перечне объектов ИТС, подлежащих защите, Исполнитель разрабатывает пакет документов «План защиты информации», который утверждается Заказчиком:

- документ «Модель угроз информации»;
- документ «Задание на создание КСЗИ»;
- документ «Политика защиты информации».

Документ «Политика защиты информации» разрабатывается после проведения Исполнителем оценки рисков и определяет защитные мероприятия, реализация которых приведет к защищенности информационных ресурсов на приемлемом уровне.

4. Разработка «Технического задания на создание КСЗИ»

На этом этапе специалисты Исполнителя разрабатывают и согласовывают с Заказчиком документ «Техническое задание на создание КСЗИ», который определяет все основные требования к КСЗИ и возможные пути реализации ее составляющих элементов.

5. Разработка «Технического проекта на создание КСЗИ»

После согласования «Технического задания на создание КСЗИ» Исполнитель разрабатывает пакет документов «Технический проект на создание КСЗИ».

«Технический проект на создание КСЗИ» представляет собой комплект документов, в который входит часть документов разработанных на предыдущих этапах и ряд новых документов, в которых описано, как именно будет создаваться, эксплуатироваться и, в случае необходимости, модернизироваться КСЗИ.

6. Приведение информационной инфраструктуры Заказчика в соответствие с «Техническим проектом на создание КСЗИ»

Особенностью этого этапа является то, что на момент принятия решения о создании КСЗИ стоимость этого этапа является неизвестной как для Заказчика, так и для Исполнителя. Также, ввиду большого возможного спектра выполнения работ, на этом этапе существует большая вероятность подключения к его выполнению Подрядчиков.

На этом этапе могут выполняться монтажные, строительные, пусконаладочные работы, работы связанные с установкой необходимых технических или криптографических средств защиты информации, средств физической защиты элементов ИТС (устанавливается необходимое оборудование и программное обеспечение, средства контроля доступа, охранная и пожарная сигнализации) и т.д.

7. Разработка «Эксплуатационной документации на КСЗИ»

На этом этапе Исполнитель КСЗИ создает пакет документов «Эксплуатационная документация на КСЗИ», который включает:

- инструкции эксплуатации КСЗИ и ее элементов;
- процедуры регламентного обслуживания КСЗИ;
- правила и положения по проведению тестирования и анализа работы КСЗИ.

8. Внедрение КСЗИ

На этом этапе Исполнитель (или Подрядчик под авторским надзором Исполнителя) проводит все пусконаладочные работы, обучает и инструктирует персонал Заказчика правилам и режимам эксплуатации КСЗИ.

После реализации этого этапа внедренная КСЗИ готова к последующему испытанию.

9. Испытание КСЗИ

На этом этапе Заказчик, при активной поддержке Исполнителя, проводит предварительные испытания КСЗИ, с целью подтверждения результативности ее работы и соответствия положениям, определенным в «Техническом задании на создание КСЗИ».

В процессе испытания выполняются тестовые задания и контролируются полученные результаты, которые и являются индикатором работоспособности спроектированной КСЗИ.

По результатам испытания КСЗИ делается вывод относительно возможности представления КСЗИ на государственную экспертизу.

10. Проведение государственной экспертизы КСЗИ и получения «Аттестата соответствия»

На этом этапе назначается организатор Государственной экспертизы, который проводит независимый анализ соответствия КСЗИ требованиям, изложенным в документе «Техническое задание на создание КСЗИ», нормативной документации по технической защите информации, а также определяет возможность введения КСЗИ в промышленную эксплуатацию.

Привлечение независимого эксперта (Организатора экспертизы) к проведению государственной экспертизы КСЗИ повышает объективность оценки проведенных работ и уменьшает риск нарушений и злоупотреблений в сфере защиты информации.

Любая организация, входящая в Реестр Организаторов экспертиз в сфере ТЗИ, может проводить экспертизы как вновь созданных КСЗИ, так и КСЗИ, «Аттестат соответствия» на которые необходимо продлевать.

По результатам проведения государственной экспертизы КСЗИ, выдается документ «Аттестат соответствия», подтверждающий качество и надежность построенной КСЗИ.

«Аттестат соответствия» является обязательным для ввода КСЗИ в промышленную эксплуатацию.

11. Поддержка и обслуживание КСЗИ

На этом этапе Исполнитель может проводить авторский надзор и оказывать консультационную помощь Заказчику в эксплуатации КСЗИ, анализе ее работы, выработок рекомендаций и, при необходимости, ее модернизации и развитии.

ТОВ «АТМНИС»
Юридический адрес: 03151, г. Киев,
ул. Керченская, 7/7
Адрес для переписки: 03035, г. Киев,
ул. Урицкого 45, оф. 928
тел: +380 44 245-64-95
www.atmnis.com