МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ПРОГРАММИРОВАНИЯ

А.В. СОЛОДЯННИКОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Учебное пособие

ИЗДАТЕЛЬСТВО
САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО
ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2020

ББК 32.965
С60

Солодянников А.В.

С60 Информационная безопасность автоматизированных систем / А.В. Солодянников. – СПб. : Изд-во СПбГЭУ, 2020. – 108 с.

ISBN 978-5-7310-5001-2

В учебном пособии рассматриваются вопросы выработки концепции, проектирования, формирования, разработки и эксплуатации автоматизированных систем в защищенном исполнении. Подробно раскрываются основные понятия, выбор способов и методов проектирования, требования к разделам и подразделам технического задания на создание систем с учетом требований по безопасности информации.

Дополнительно затронуты проблемы проведения аттестации и сертификации автоматизированных систем в Системе сертификации средств защиты информации по требованиям безопасности информации в непростых условиях рыночной экономики.

Предназначено для бакалавров направления подготовки 10.03.01 «Информационная безопасность», а также может представлять интерес для всех изучающих данную и смежные дисциплины.

The tutorial discusses the issues of conceptual approach to the design, formation, development and operation of automated systems in a secure performance. Details the basic concepts, selection of methods and design techniques, requirements, sections and subsections of the technical specification for development of systems requirements for information security.

In addition, the problems of certification and certification of automated systems in the system of certification of information security according to the requirements of information security in difficult conditions of the market economy are touched upon.

The manual is intended for bachelors of training 10.03.01 "Information security", and may also be of interest to all students of this and related disciplines.

ББК 32.965

Рецензенты: д-р экон. наук, проф. **Е.В. Стельмашонок**
канд. техн. наук, доц. **Г.М. Чернокнижный**

ISBN 978-5-7310-5001-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие информационных технологий, трансграничное их проникновение и использование во всех сферах деятельности современного человека выдвинули целый ряд новых проблем, требующих незамедлительного решения. Сегодня нет предприятий, фирм, организаций или отдельных пользователей ПЭВМ, которые бы не ставили периодически перед собой задачу защиты информации или работоспособности технических средств. Проблема информационной безопасности из разряда узкоспециальных и доступных только профессионалам становится жизненно важной для подавляющего круга населения страны. Задача защиты информации, в силу разнообразия объектов защиты, становиться комплексной. Решение этой комплексной задачи предусматривает реализацию множества мероприятий: правовых, программно-аппаратных, криптографических, технических и организационных. Для этого необходима концепция решения проблемы проектирования, разработки, формирования и внедрения автоматизированных систем в защищенном исполнении.

В настоящее время в ряде вузов осуществляется подготовка бакалавров и специалистов по направлению «Информационная безопасность».

В предлагаемом учебном пособии сделан акцент на обобщении материалов при построении автоматизированных систем (АС), описании подходов к проектированию, формированию, внедрению и сопровождению подсистем защиты информации (ЗИ) в составе АС. Материалы могут быть полезны при практической работе специалистам, студентам, абитуриентам, работающим в области защиты информации.

Подготовленное учебное пособие призвано сформировать основы системного мышления при изучении специальных дисциплин по направлению защиты информации.

Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА АВТОМАТИЗИРОВАННЫХ СИСТЕМ

1.1. Определение автоматизированной системы

Многообразие задач, решаемых с помощью ЭВМ, привело к появлению множества различных типов систем, отличающихся принципами построения и заложенными в них правилами обработки информации.

Система (Греч. "целое, составленное из частей, соединение") - это совокупность элементов, связанных между собой определенными отношениями и образующих определенную целостность, единство.

Под системой понимают любой объект, который одновременно рассматривается и как единое целое, и как совокупность объединенных в интересах достижения поставленных целей множества разнородных элементов. Системы различаются как по составу, так и по основным целям. Функционирование совокупности элементов или частей, связанных между собой и с внешней средой, направлено на получение конкретного полезного результата. Например, можно назвать системы образования, энергетики, транспорта, экономики и многие другие.

В информатике понятие "система" широко распространено и имеет множество значений. Чаще всего он используется для обозначения набора технических средств и программ.

Система должна быть гибкой, чтобы иметь возможность реагировать на изменяющиеся условия. Для этого используются различные технологии автоматизации элементов системы, да и самой системы в целом.

Автоматизация-это комплекс мероприятий и мероприятий технического, организационного и экономического характера. Это позволяет снизить степень участия, а также полностью исключить непосредственное участие человека в осуществлении производственного или иного технологического процесса.

В целом автоматизация означает использование технических средств и технологий для выполнения любых процессов с их помощью. Она служит основой для фундаментальных изменений в любых предметных областях (в производстве, управлении, обучении, культуре и др.).

Основными задачами автоматизации являются:

* снижение трудозатрат в традиционных процессах и операциях;
* устранение рутинных операций;
* ускорение процессов обработки и преобразования информации;
* расширение возможностей статистического анализа и повышение точности бухгалтерской и отчетной информации;
* повышение эффективности и качества обслуживания пользователей;

* модернизация или полная замена элементов традиционных технологий;

* расширение возможностей организации и эффективное использование информационных ресурсов организации за счет применения новых информационных технологий-штрихового кодирования, RFID, RAID, CD и DVD, систем теле-доступа и телекоммуникаций, электронной почты, других сервисов Интернета, гипертекстовых, полнотекстовых и графических машиночитаемых данных и др.;

* создание возможностей для широкого обмена информацией, предоставления услуг, эффективного участия в системах сотрудничества и интеграции.

Добавление термина " автоматизированная "к понятию" система " отражает способы создания и функционирования такой системы.

Автоматизированная система (по ГОСТу) - это система, состоящая из взаимосвязанного набора организационных единиц и набора средств автоматизации, реализующих автоматизированные функции для отдельных видов деятельности.

Компонент автоматизированной системы (АС) рассматривается как элемент одного из видов программного обеспечения (технического, программного, информационного и др.), который выполняет определенную функцию в подсистеме as и обеспечивает ее функционирование.

Перед созданием АС человек организует программу подготовительных мероприятий, поэтому требуется, в частности, специальная организационно-правовая поддержка.

В связи с производственными процессами объект и орган управления представляют собой единую человеко-машинную систему, и человек обязательно включается в схему управления.

По определению, автоматизированная система-это человеко-машинная система, предназначенная для сбора и обработки информации, необходимой для управления производственным процессом, то есть для управления коллективами людей.

Существует четыре типа автоматизированных систем:

- Охват одного процесса (операции) в организации.
- Объединение нескольких процессов в организации.
- Обеспечение функционирования единого процесса в масштабе нескольких взаимодействующих организаций.
- Реализация работы нескольких процессов или систем в масштабе нескольких организаций.

Под автоматизацией предприятий понимается не только приобретение компьютеров и создание корпоративной сети, но и создание информационной системы, включающей компьютеры, программное обеспечение и

сети, а главное – организацию информационных потоков. Разнообразные автоматизированные системы, широко применяемые в различных областях человеческой деятельности, являются информационными системами. Добавление термина "информация" к понятию "система" отражает цель ее создания и функционирования.

Информационная система-это взаимосвязанный набор инструментов, методов и персонала, используемых для хранения, обработки и выдачи информации в целях достижения поставленной цели.

Под информационной системой понимается организационно упорядоченная совокупность массивов документов и информационных технологий, в том числе с использованием вычислительной техники и средств связи, реализующих информационные процессы.

В то же время следует отметить, что под информационными процессами понимаются процессы сбора, обработки, накопления, хранения, поиска, передачи и распространения информации.

Основной целью информационной системы является производство и распространение профессиональной информации. Информационные системы обеспечивают сбор, хранение, обработку, поиск, доставку информации, необходимой в процессе решения задач из любой области. Они помогают анализировать проблемы и создавать новые продукты. Они предназначены для длительного хранения, обеспечения эффективного поиска и передачи информации по соответствующим запросам. В этом смысле их обычно называют системами обработки и хранения информации.

Информационная система является системой информационного обслуживания пользователей и выполняет технологические функции по накоплению, хранению, передаче и обработке информации. Она формируется и функционирует в нормативных актах, определяемых методами и структурой, принятыми в конкретной предметной области и даже на конкретном объекте, реализуя стоящие перед ней цели и задачи.

Совокупность информации о любом объекте называется информационной базой. Информационная база присуща любому объекту независимо от уровня техники управления. Он делится на подсистемы, массивы, индикаторы, детали. Массив-это структурная единица информации, представляющая собой набор данных, связанных с одной задачей (подсистемой).

Информационная база, записанная на машинных (электронных) носителях информации и используемая для решения задач на компьютере, называется базой данных.

Информационная база является основой внутримашинного информационного обеспечения, это совокупность всех данных, подлежащих накоплению, хранению, поиску, преобразованию, доставке в установленном порядке, а также использованию для организации связи человека с компьютером.

База данных - это управляемый набор данных, который является исходной информацией для решения управленческих задач и принятия управленческих решений. База данных может содержать информацию по всем задачам, решаемым в автоматизированных системах, или по группам задач.

Обработка и выдача необходимой информации для группы пользователей или задач управления осуществляется с помощью программ управления информационной базой.

Система управления базами данных представляет собой набор языковых и программных средств, обеспечивающих формирование и ведение электронных наборов данных.

Любая информационная система предполагает участие людей в ее работе. Среди персонала, связанного с информационными системами, есть такие категории, как конечные пользователи, программисты, системные аналитики, администраторы баз данных и др.

Системный аналитик-это человек, который оценивает потребности пользователей в применении компьютера, а также разрабатывает информационные системы, удовлетворяющие этим потребностям.

Специалисты по обработке данных профессионально анализируют, проектируют и разрабатывают систему.

Человек, использующий результат компьютерной программы, называется конечным пользователем.

Конечным пользователем является лицо или любое другое живое существо, использующее информационную систему или содержащуюся в ней информацию.

Информационные системы существуют уже сотни лет и используются на практике в виде различных картотек и коллекций бумажных документов. Однако в таких системах отсутствует автоматизация обработки данных. Они позволяют только регистрировать и сохранять в систематическом виде на бумаге результаты натурных измерений. Современное понимание информационной системы предполагает использование компьютера Как основного технического средства обработки информации. В результате такие системы становятся автоматизированными.

Автоматизированная информационная система - это совокупность программно-технических средств, предназначенных для хранения и (или) управления данными и информацией, а также для производства расчетов.

Это человеко-машинная система, обеспечивающая автоматизированную подготовку, поиск и обработку информации в рамках интегрированных сетевых, компьютерных и коммуникационных технологий для оптимизации деятельности в различных предметных областях и сферах управления.

1.2. Характеристики автоматизированных систем

Автоматизированная система, сокращенно - это система, включающая в себя объект управления и системы управления, некоторые функции в таких системах возложены на человека. АС-это организационно-техническая система, обеспечивающая разработку решений на основе автоматизации информационных процессов в различных отраслях промышленности (производство, управление, проектирование, экономика).

Все функции автоматизированных систем направлены на достижение определенной цели посредством определенных действий и действий. Основной целью АС является максимально эффективное использование возможностей и функций объекта управления.

Существуют следующие цели создания автоматизированных систем:

- Предоставление соответствующих данных, необходимых для принятия решений.
- Более быстрый и эффективный сбор и обработка информации.
- Сокращение числа решений, которые должен принимать орган, принимающий решения (ЛПР).
- Повышение уровня контроля и дисциплины.
- Оперативное управление.
- Снижение затрат ЛНР на реализацию технологических процессов.
- Обоснованные решения.
- Классификация автоматизированных систем
- Выявлены основные признаки, по которым осуществляется классификация автоматизированных систем:
- Сфера, в которой функционирует объект управления: строительство, промышленность, непромышленная сфера, сельское хозяйство.
- Тип рабочего процесса: организационный, экономический, производственный.
- Уровень в системе государственного управления.

Категории автоматизированных систем.

Классификация структур автоматизированных систем в промышленной сфере подразделяется на следующие категории:

Децентрализованная структура. Система с такой структурой используется для автоматизации независимых объектов управления и является наиболее эффективной для этих целей. Система представляет собой комплекс независимых систем с индивидуальным набором алгоритмов и информации. Каждое выполняемое действие выполняется исключительно для своего объекта управления.

Централизованная структура. Реализует все необходимые процессы управления в единой системе, которая собирает и структурирует информа-

цию об объектах управления. На основании полученной информации система делает выводы и принимает соответствующее решение, которое направлено на достижение первоначальной цели.

Централизованная дисперсная структура. Структура работает на принципах централизованного управления. По каждому объекту управления разрабатываются управляющие воздействия на основе данных по всем объектам. Некоторые устройства могут совместно использоваться каналами.

Алгоритм управления основан на наборе общих алгоритмов управления, реализованных с использованием набора связанных объектов управления. В процессе работы каждый орган управления получает и обрабатывает данные, а также передает управляющие сигналы на объекты. Преимуществом структуры является не столь строгие требования в отношении производительности процессинговых центров и управления, не наносящие ущерба процессу управления.

Иерархическая структура. В связи с увеличением количества задач в управлении сложными системами, разрабатываемые алгоритмы значительно усложняются. В результате возникает необходимость в создании иерархической структуры. Такое формирование значительно снижает трудности управления каждым объектом, однако необходимо согласовывать их решения.

Типы автоматизированных систем.

В зависимости от выполняемых функций АИС различают следующие типы автоматизированных систем:

- АСУП-системы управления предприятием.
- Система управления технологическими процессами – системы управления технологическими процессами.
- ASUPP-системы подготовки производства.
- ОАС-системы управления отраслью.
- организационно-распорядительные.
- АСК-системы контроля качества продукции.
- GPS-гибкие производственные системы.
- Системы управления CNC-машины с численным программным обеспечением.
- группа систем или интегрированная система.

Автоматизированная информационная система.

Автоматизированная информационная система - это совокупность аппаратных и программных средств, необходимых для реализации функций хранения и управления данными, а также для выполнения вычислительных операций.

Основным назначением АИС является хранение данных, обеспечивающее качественный поиск и передачу данных в зависимости от запросов для максимального соответствия запросам пользователей.

Наиболее важные принципы автоматизации технологических процессов:

- надежность;
- полная окупаемость;
- гибкость;
- безопасность;
- соответствие стандартам;
- дружелюбие.

Классификация автоматизированных информационных систем имеет следующую структуру:

- Система, которая охватывает один процесс в организации.
- С организацией осуществляется несколько процессов.
- Нормальное функционирование одного процесса в нескольких взаимосвязанных организациях.
- Система, которая организует функционирование нескольких процессов в нескольких взаимосвязанных системах.

Классификация по степени автоматизации.

Информационные системы также классифицируются по степени автоматизации операций:

- руководство;
- автоматизированный;
- автомат.

Ручные-у них нет современных средств обработки информации, и все операции выполняются человеком в ручном режиме.

Автоматическая-абсолютно все операции по обработке информации осуществляются с использованием технических средств без вмешательства человека.

Автоматизированные информационные системы выполняют операции как с помощью технических средств, так и с помощью человека, однако основная роль переносится на компьютер. ИС классифицируется по степени автоматизации, а также по объему и характеру деятельности.

Уровни автоматизированных систем.

Существует три уровня автоматизированных систем управления :

Нижний уровень. Оборудование. На этом уровне внимание уделяется датчикам, измерительным и исполнительным механизмам. Здесь сигналы координируются с входами устройств, а команды-с исполнительными механизмами.

Средний уровень. Уровень контроллера. Контроллеры получают данные от измерительного оборудования, а затем передают сигналы для команд управления, в зависимости от запрограммированного алгоритма.

Верхний уровень-промышленные серверы и станции управления. Здесь осуществляется производственный контроль. Для этого обеспечивается связь с нижестоящими уровнями, сбор информации и мониторинг технологического процесса. Этот уровень взаимодействует с человеком. Человек здесь осуществляет управление оборудованием с помощью человеко-машинного интерфейса: графических панелей, мониторов. Управление системой станка обеспечивается системой SCADA, которая устанавливается на управляющие компьютеры. Эта программа собирает информацию, архивирует ее и визуализирует. Программа самостоятельно сравнивает полученные данные с заданными показателями и в случае расхождения уведомляет человека-оператора об ошибке. Программа записывает все операции, включая действия оператора, которые необходимы в случае возникновения чрезвычайной ситуации. Это обеспечивает контроль ответственности оператора.

Существуют также критические автоматизированные системы. Это системы, реализующие различные информационные процессы в критических системах управления. Критичность-это вероятный риск нарушения их стабильности, а выход из строя системы чреват значительным экономическим, политическим или иным ущербом.

Что относится к критическим автоматизированным процессам? К критическим относятся следующие системы управления: опасные отрасли промышленности, ядерные объекты, управление космическими полетами, железнодорожным движением, воздушным движением, управление в военно-политической сфере. Почему они критичны? Потому что решаемые ими задачи критичны: использование информации с ограниченным доступом, использование биологических и электронных средств обработки информации, сложность технологических процессов. Следовательно, информационные автоматизированные системы становятся элементом критических систем управления и, как следствие, получили принадлежность к этому классу.

Глава 2. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

2.1. Требования проведения аудита

Аудит информационной безопасности – это всестороннее обследование, позволяющее оценить текущее состояние информационной безопасности организации и спланировать дальнейшие шаги по повышению уровня защищенности.

Основная задача - объективно оценить текущее состояние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности компании.

Сущность аудита на соответствие системы информационной безопасности компании требованиям стандарта заключается в проверке выполнения каждого положения стандарта ISO 17799. По каждому такому положению проверяющие должны ответить на два вопроса: выполняется ли данное требование, и если нет, то каковы причины невыполнения?

В практических рекомендациях Британского института стандартов BSI отмечается, что в среднем трудоемкость аудита информационной безопасности средней и крупной компаний может составлять 30-45 человекодней работы аудитора. По результатам успешно выполненного аудита компании или ее информационной системы и подсистемы информационной безопасности осуществляется выдача сертификатов на соответствие стандарту ISO/IEC 17799:2000 (BS 7799-1:2000), которые считаются действительными в течение 3 лет.

Под аудитом понимается комплекс работ, включающий исследование всех аспектов обеспечения информационной безопасности в организации, проводимое по согласованному с заказчиком плану, в соответствии с выбранной методикой и критериями.

Аудит информационной безопасности - один из наиболее эффективных сегодня инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Результаты аудита дают основу для формирования стратегии развития системы обеспечения информационной безопасности организации. Необходимо понимать, что аудит безопасности - не разовая процедура, он должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности компании.

Аудит информационной безопасности целесообразно проводить в случаях, когда нужна актуальная информация и независимая оценка состояния информационной безопасности.

Необходимость в этом может возникнуть в разных ситуациях:

– если меняется стратегия компании;

– при слиянии или поглощении;

– когда происходят значительные изменения в организационной структуре или смена руководства;

– при появлении новых внутренних или внешних требований в области информационной безопасности;

– в случае значительных изменений бизнес-процессов или ИТ-инфраструктуры.

Аудит может проводиться как для компании в целом, так и для отдельных критичных областей, бизнес-процессов или информационных систем.

Работа проводится экспертами, обладающими квалификацией и богатым опытом проведения аудитов в различных отраслях экономики.

Методика выполнения работ предполагает гибкость и индивидуальный подход, позволяет учесть специфичные требования и особенности бизнеса каждой конкретной организации.

2.2. Этапы проведения аудита

2.1.1 Работы по аудиту безопасности включают в себя ряд последовательных этапов, которые в целом соответствуют этапам проведения комплексного аудита, включающего:

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- выработка рекомендаций;
- подготовка аудиторского отчета.

2.1.2 Создание приказа о проведении аудита.

Приказ о проведении внутренней проверки определяет положение о проведении внутренней проверки.

Приказ должен:

• Быть оформлен в соответствии с внутренним порядком документооборота Учреждения.

• Быть утвержден Руководителем Предприятия.

• В приказе должен быть установлен срок проведения проверки.

• В приказе должен быть указан состав комиссии по классификации ИСПДн. В состав комиссии рекомендуется включить ответственного за обеспечение безопасности, руководителей отделов, чьи подразделения

участвуют в обработке персональных данных, технических специалистов, обеспечивающих поддержку технических средств. Также к участию в комиссии в качестве консультантов можно привлекать специалистов сторонних организаций.

• В приказе должен быть указан сотрудник ответственный за контроль исполнения приказа.

• Ответственным сотрудником может быть Руководитель Предприятия, лицо, отвечающее за обеспечение режима безопасности или проведение внутренней проверки, или любой другой сотрудник, на которого возложен контроль за выполнение приказа.

Задачи внутренней проверки представлены на рисунке 1.

Рисунок 1. Задачи проверки

2.1.3 Рекомендации по сбору исходных данных.

Для проведения классификации информационных систем необходимо провести мероприятия по сбору и анализу исходных данных по

информационной системе и обрабатываемых в ней ПДн, а также провести их инвентаризацию.

При проведении обследования информационных систем по критериям наличия указанной информации руководством принимается решение об обработке в данной информационной системе персональных данных. Решение принимается на основании **Отчета о результатах проведения внутренней проверки.**

Объекты защиты каждой ИСПДн включают:

- Обрабатываемая информация:
  - персональные данные субъектов ПДн;
  - персональные данные сотрудников;
- Технологическая информация.
- Программно-технические средства обработки.
- Средства защиты ПДн.
- Каналы информационного обмена и телекоммуникации.
- Объекты и помещения, в которых размещены компоненты ИСПДн.

Этап сбора информации аудита, является наиболее сложным и длительным. Это связано с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

Компетентные выводы относительно положения дел с информационной безопасностью могут быть сделаны аудитором только при условии наличия всех необходимых исходных данных для анализа.

Получение информации о функционировании и текущем состоянии ИСПДн осуществляется аудитором в ходе специально организованных интервью с ответственными лицами компании, путем изучения технической и организационно-распорядительной документации, а также исследования ИСПДн с использованием специализированного программного инструментария.

Понятие инвентаризации.

- Инвентаризация информационных ресурсов - это процедура анализа хранимой и обрабатываемой на объекте информатизации информации в интересах отнесения ее к защищаемой, разделения защищаемой информации на именованные блоки с обеспечением возможности нахождения любого блока по его имени при решении задач защиты, а также определение носителей защищаемой информации.
- Категорирование защищаемой информации - это присвоение именованному блоку информации соответствующей категории из заранее определенного списка категорий

Алгоритм инвентаризации представлен на рисунках 2.1 , 2.2.

Рис. 2.1 Алгоритм инвентаризации информационных ресурсов.

Рис. 2.2 Алгоритм инвентаризации информационных ресурсов (продолжение)

2.3. Содержание аудита безопасности

2.1.4 Исследование и оценка состояния информационной безопасности:

- на соответствие типовым требованиям РД ФСТЭК России
- на соответствие типовым требованиям международных стандартов ISO
- на соответствие специальным требованиям предприятия

2.1.5 Работы на основе анализа рисков:

- качественный и количественный анализ рисков
- оценка организации управления рисками на основе их оценок

2.1.6 Инструментальные исследования:

- исследование элементов инфраструктуры корпоративной информационной системы на наличие уязвимостей
- исследование защищенности точек доступа предприятия в Internet

2.1.7 Анализ документооборота предприятия.

Аудит позволяет получить ответы на следующие вопросы.

- Соответствует ли система информационной безопасности целям и задачам бизнеса компании?
- Насколько адекватна принятая в компании политика безопасности ее задачам и целям бизнеса?
- Как корректно контролировать реализацию и выполнение политики безопасности в компании?
- Когда и как необходимо провести модернизацию системы безопасности и затрат?
- Как быстро окупятся инвестиции в систему безопасности?
- Насколько правильно и корректно сконфигурированы и настроены штатные средства обеспечения информационной безопасности компании?
- Как убедиться в том, существующие средства защиты эффективно справляются со своими задачами?
- Как решаются вопросы обеспечения конфиденциальности, доступности и целостности?
- Как оценить работу подрядных организации, производивших проектирование, поставку, монтаж, пуско-наладку средств безопасности.
- Как обеспечить "вертикаль власти" для централизованного управления безопасностью компании?
- Какие методы и средства использовать для контроля состояние информационной безопасности компании?
- Что делать после того, как система обеспечения безопасность построена, дальше? (Наличие стратегического и тактических планов защиты, планов работы при возникновении чрезвычайных ситуаций).

• Если есть необходимость, то какие бюджетные средства необходимо тратить на обучение сотрудников службы информационной безопасности компании?

• Как управлять информационными рисками компании? Какие инструментальные средства для этого необходимо задействовать?

• Удовлетворяет ли организация информационной безопасности компании требованиям международных стандартов оценки и управления безопасностью, например ISO 15408, ISO 17799?

В процессе аудита проводятся:

– анализ организационно-распорядительных документов организации;

– интервью с сотрудниками организации: представителями бизнес-подразделений, администраторами и разработчиками информационных систем, специалистами по информационной безопасности;

– осмотр технологических и офисных помещений с точки зрения обеспечения физической безопасности ИТ-инфраструктуры;

– анализ конфигурационных настроек оборудования и ПО;

– аудит с использованием специальных технических средств (сканеров анализа защищенности, средств контроля утечек информации и т.п.);

– тестирование на проникновение;

– оценка знаний сотрудников организации в области информационной безопасности.

Также могут быть выполнены дополнительные специальные проверки, позволяющие учесть особенности организации, в которой проводится аудит.

2.1.8 Обобщенное содержание работ по аудиту.

Проведение аудита (инвентаризации) деятельности оператора на предмет наличия/отсутствия признаков организации работы с персональными данными включает:

Составление опросных листов, учитывающих специфику деятельности оператора, на базе типовых опросных листов;

Обработку полученной информации, включая предоставленные Заказчиком, локальные нормативные правовые акты, регулирующие (затрагивающие) вопросы обработки персональных данных у Заказчика;

Подготовку раздела аналитического отчета о состоянии дел по организации работы с персональными данными с указанием на недостатки в организации такой работы, и предложением типовых решений для нормализации ситуации.

Моделирование бизнес-процессов Заказчика по организации работы с персональными данными клиентов. Моделирование бизнес-процессов включает:

Выявление бизнес-процессов Заказчика по организации работы с персональными данными, и/или бизнес-процессов, затрагивающих вопросы персональных данных;

Анализ организационной структуры Заказчика, включая анализ функций структурных подразделений, на которые возложена работа с персональными данными;

Подготовку раздела аналитического отчета, содержащего моделирование бизнес-процессов Заказчика по организации работы с персональными данными клиентов. При этом учитывается специфика деятельности оператора, существующая нормативная правовая база, регулирующая сферу деятельности оператора и практика работы Заказчика с персональными данными клиентов.

Разработка локальной нормативной правовой базы Заказчика по организации работы с персональными данными включает:

Построение модели нормативного правового обеспечения деятельности Заказчика по организации работы с персональными данными, учитывающей специфику деятельности Заказчика и существующие бизнес-процессы;

Выявление локальных нормативных правовых актов Заказчика, регулирующих/затрагивающих вопросы персональных данных, анализ их содержания;

Подготовку раздела аналитического отчета, включающего описание состояния дел Заказчика по нормативному правовому регулированию организации работы с персональными данными, проекты необходимых, но отсутствующих у Заказчика документов, либо предложения по изменению и/или дополнению уже существующих документов, регулирующих вопросы работы с персональными данными.

2.1.9 Результаты аудита:

– анализ угроз, которые могут быть реализованы, через обнаруженные уязвимости;

– качественная или количественная оценка рисков ИБ;

– оценка соответствия актуальным требованиям;

– оценка соответствия лучшим практикам и стандартам в области ИБ;

– стратегия обеспечения ИБ;

– рекомендации, которые должны быть выполнены для повышения уровня защищенности организации;

– план реализации разработанных рекомендаций с бюджетной оценкой;

– техническое задание на внедрение рекомендуемых мер по обеспечению информационной безопасности.

В случае необходимости на этапе обследования может быть собрана дополнительная информация, необходимая для выполнении других проектов, что позволит в дальнейшем сэкономить ресурсы организации и равномерно распределить расходы бюджета.

2.4. Перечень исходных данных, необходимых для проведения аудита

В процессе аудита выявляются особенности эксплуатации изделия в реальных условиях эксплуатации. На начальном этапе проводится опрос и формируется перечень ответов.

Для проведения аудита аудитору может потребоваться дополнительная информация.

Аудитору требуется следующая документация:

- схема организационной структуры пользователей;
- схема организационной структуры обслуживающих подразделений;
- структурная схема ИС;
- схема информационных потоков;
- описание структуры комплекса технических средств информационной системы;
- описание структуры программного обеспечения;
- описание структуры информационного обеспечения;
- размещение компонентов информационной системы;
- функциональные схемы;
- описание автоматизированных функций;
- описание основных технических решений;
- другая проектная и рабочая документация на информационную (телекоммуникационную) систему.

Подготовка значительной части документации на ИС, обычно, осуществляется уже в процессе проведения аудита. Когда все необходимые данные по ИС, включая документацию, подготовлены, можно переходить к их анализу.

Обычно, в ходе интервью аудитор задает опрашиваемым следующие вопросы:

- кто является обладателем информации;
- кто является пользователем (потребителем) информации;
- кто является провайдером услуг;
- назначение и принципы функционирования ИС;
- какие услуги, и каким образом предоставляются конечным пользователям;
- какие основные виды приложений, функционирует в ИС;

- количество и виды пользователей, использующих эти приложения;
- из каких компонентов (подсистем) состоит ИС;
- функциональность отдельных компонент;
- где проходят границы системы;
- какие точки входа имеются;
- как ИС взаимодействует с другими системами;
- какие каналы связи используются для взаимодействия с другими ИС;
- какие каналы связи используются для взаимодействия между компонентами системы;
- по каким протоколам осуществляется взаимодействие;
- какие программно-технические платформы используются при построении системы.

Перечень вопросов приведен в таблице 1.

Таблица 1 – Перечень вопросов при проведении первичного аудита

№ п/п		да	нет
1	Наличие сведений ограниченного доступа		
2	Наличие перечня сведений, ограниченного доступа.		
3	Наличие объектов, на которых осуществляется обработка защищаемой информации.		
4	Перечень ТС, на которых осуществляется обработка защищаемой информации.		
5	План границ контролируемой территории.		
6	Исходные данные об ИТ-структуре		
	- организация сетевой инфраструктуры информационной сети;		
	- территориальное размещение объектов (топология сети);		
	- физические связи объектов, в том числе с сетями общего пользования;		
	- функциональные и технологические связи внутри объекта и с другими системами;		
	- информация о серверных платформах;		
	- перечень АРМ, входящих в объект;		
	- перечень системного, прикладного ПО, входящего в состав объекта;		
	- перечень средств защиты информации, реализованных на объекте;		
7	Наличие системы документации по СЗИ;		
8	Степень конфиденциальности обрабатываемой информации.		
9	Наличие модели угроз, модели нарушителя.		
10	Наличие обученного(необученного персонала).		
11	Необходимость проведения обучения.		

2.5. Требования к аккредитации компаний, занимающихся аудитом информационной безопасности

В соответствии с требованиями законодательства РФ, любая организация, использующая в своей деятельности какие-либо конфиденциальные данные, обязана обеспечивать безопасность их обработки и хранения.

Аудит информационной безопасности позволяет получить независимую качественную и количественную оценку защищенности корпоративной информационной системы, оценить ее соответствие предъявляемым нормативным и корпоративным требованиям безопасности.

Аудит информационной безопасности включает:

- Анализ защищенности информационных систем;
- Анализ угроз нарушения информационной безопасности;
- Оценку информационных рисков и воздействия на бизнес;
- Оценку соответствия требованиям стандартов;
- Аттестацию и сертификацию по требованиям безопасности информации РД ФСТЭК России.

Зачастую компании не имеют собственных квалифицированных специалистов, способных провести оценку имеющейся информационной системы, и отдают этот вид деятельности на аутсорсинг.

Прежде чем заниматься аудитом информационной безопасности, организация должна пройти аккредитацию на проведение сертификационной оценки.

Еще несколько лет назад не существовало четких требований к компаниям, осуществляющим аудит информационной безопасности.

В данной статье рассмотрены основные требования к аккредитации организаций, предоставляющих услуги аудита информационной безопасности, существующие в настоящее время.

В первую очередь компания должна иметь лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

Под технической защитой конфиденциальной информации понимается выполнение работ или оказание услуг, определенных Постановлением Правительства РФ от 3 февраля 2012 г. № 79, в том числе аттестационные испытания и аттестация на соответствие требованиям по защите информации.

На сайте ФСТЭК можно найти и скачать реестр лицензий на деятельность по технической защите конфиденциальной информации, который содержит номера выданных лицензий, дату выдачи, срок действия, наименование лицензиата, адрес места нахождения и осуществления деятельности.

Лицензия ФСТЭК требует наличия у организации действующей лицензии ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну.

Также организация, занимающаяся аудитом информационной безопасности должна осуществлять свою деятельность в соответствии со стандартом ГОСТ Р ИСО/МЭК 27006-2008 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

Данный стандарт устанавливает требования к организациям, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности. Он также может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки и других процессов аудита.

Требования ГОСТа Р ИСО/МЭК 27006-2008 содержат нормативные ссылки на следующие стандарты:

- ИСО/МЭК 17021:2006 «Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента»;
- ИСО/МЭК 27001:2005 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ИСО/МЭК 19011:2002 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента».

Одной из важных особенностей стандарта является наличие требований к компетентности персонала компании, занимающейся аудитом информационной безопасности.

- Знание стандарта СМИБ и других соответствующих нормативных документов;
- Понимание вопросов информационной безопасности;
- Понимание оценки риска и менеджмента риска с точки зрения деятельности;
- Технические знания о деятельности, подлежащей аудиту;
- Общие знания нормативных требований, относящихся к СМИБ;
- Знание систем менеджмента;
- Понимание принципов аудита, основанных на ИСО 19011:2002;
- Знание анализа эффективности СМИБ и измерения эффективности средств контроля.

Для компаний, занимающихся аудитом информационной безопасности банков, являются существенными следующие документы:

- Комплекс документов Банка России СТО БР ИББС;
- Стандарт PCI DSS;
- Федеральный Закон от 27 июня 2011 г. № 161 –ФЗ «О национальной платёжной системе».

Стандарт СТО БР ИББС описывает единый подход к построению системы обеспечения информационной безопасности организаций банков-

ской сферы с учетом требований российского законодательства. Вопросы аудита и оценки соответствия требованиям стандарта прописаны в отдельных документах — «СТО БР ИББС-1.1-2007. Аудит информационной безопасности», «СТО БР ИББС-1.2-2010. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2010» и «РС БР ИББС-2.1-2007. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

Стандарт PCI DSS (PaymentCardIndustryDataSecurityStandard)- стандарт безопасности данных платежных карт, разработанный Советом по стандартам безопасности индустрии платежных карт (PaymentCardIndustry SecurityStandardsCouncil, PCI SSC), который был учрежден международными платежными системами Visa, MasterCard, AmericanExpress, JCB и Discover. Стандарт PCI DSS представляет собой совокупность 12 высокоуровневых и свыше 200 детальных требований по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационных системах организаций. Требования стандарта распространяются на все компании, работающие с международными платежными системами Visa и MasterCard.

Законодательство о национальной платежной системе (НПС) находится только на заре своего становления. Согласно данному федеральному закону оценка соответствия похожа по своей сути на то, что описано в методике оценки соответствия СТО БР ИББС, но выдает совершенно иные результаты. Это связано с вводом специальных корректирующих коэффициентов, которые и определяют отличающиеся результаты.

2.6. Содержание отчета по результатам аудита

Аннотация.

Основные термины и определения.

ОБЩИЕ ПОЛОЖЕНИЯ

- Модель защиты ИСПДн.

- Методология поиска уязвимостей ИСПДн, построения модели нарушителя, анализа угроз безопасности и риска потерь.

- Рекомендации по использованию отчета.

ОПИСАНИЕ ФАКТИЧЕСКОГО СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИСПДн

- Состояние организационно-правового обеспечения безопасности ИСПДн.

- Состояние перечня и содержания документов регламентирующих порядок создания, функционирования и модернизации системы безопасности ИСПДн.

- Состояние кадрового обеспеченья безопасности автоматизированной системы предприятия, степень готовности персонала к решению задач защиты информации.

- Состояние режима сохранности информации конфиденциального характера в автоматизированной системе и на машинных носителях.

- Состояние программно-аппаратного обеспечения автоматизированной системы предприятия и системы защиты информации.

- Структура и топология сети ЭВМ предприятия, установленные средства защиты.

- Аппаратное обеспечение автоматизированной системы предприятия и системы защиты информации, состав, порядок использования и режимы работы.

- Программное обеспечение автоматизированной системы предприятия и системы защиты информации, сервисы и службы сети ЭВМ.

- Порядок и правила доступа к Internet.

- Состав и структура потоков конфиденциальной информации и информации общего доступа циркулирующих в автоматизированной системе предприятия.

Рекомендации по разработке отчета.

Состояние кадрового обеспеченья безопасности автоматизированной системы предприятия, степень готовности персонала к решению задач защиты информации.

Состояние режима сохранности информации конфиденциального характера в автоматизированной системе и на машинных носителях.

Состояние программно-аппаратного обеспечения автоматизированной системы предприятия и системы защиты информации.

Структура и топология сети ЭВМ предприятия, установленные средства защиты.

Аппаратное обеспечение автоматизированной системы предприятия и системы защиты информации, состав, порядок использования и режимы работы.

• Программное обеспечение автоматизированной системы предприятия и системы защиты информации, сервисы и службы сети ЭВМ. Для каждой ИСПДн должны быть определены имеющиеся организационные меры защиты. Перечень возможных организационных мер представлен в Плане мероприятий по обеспечению защиты ПДн.

• Для каждой ИСПДн должны быть определены необходимые меры по снижению опасности актуальных угроз. Анализ актуальности угроз производится на основании Методических рекомендаций по составлению модели угроз.

• Перечень возможных организационных мер представлен в Плане мероприятий по обеспечению защиты ПДн.

Порядок и правила доступа к Internet.

Состав и структура потоков конфиденциальной информации и информации общего доступа циркулирующих в автоматизированной системе предприятия.

Типовая технологическая информация, подлежащая защите.

Технологическая информация, подлежащая защите, включает:

• управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

• технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

• информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

• информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

• информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

• служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

Глава 3. ОСОБЕННОСТИ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

3.1. Требования к защищенным автоматизированным системам

Для обработки информации, необходимость защиты которой определяется законодательством Российской Федерации или решением ее обладателя, должны создаваться АСЗИ, в которых реализованы в соответствии с действующими нормативными правовыми актами требования о ЗИ. Реализация требований о ЗИ в АСЗИ осуществляется системой ЗИ, являющейся неотъемлемой составной частью АСЗИ.

Целью создания системы ЗИ АСЗИ является обеспечение ЗИ от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа, реализация права на доступ к информации.

При создании (модернизации) АСЗИ необходимо руководствоваться следующими общими требованиями:

- система ЗИ АСЗИ должна обеспечивать комплексное решение задач по ЗИ от НСД, от утечки защищаемой информации по техническим каналам, от несанкционированных и непреднамеренных воздействий на информацию (на носители информации) применительно к конкретной АСЗИ. Состав решаемых задач по ЗИ определяется задачами обработки информации, решаемыми с использованием АСЗИ, ее программным и аппаратным составом, конфигурацией этой системы, условиями функционирования, требованиями, предъявляемыми к обрабатываемой информации, угрозами безопасности информации;
- система ЗИ АСЗИ должна разрабатываться (проектироваться) с учетом возможности реализации требований о защите обрабатываемой информации при использовании в АСЗИ методов и программно-аппаратных средств организации сетевого взаимодействия;
- система ЗИ АСЗИ должна создаваться с учетом обеспечения возможности формирования различных вариантов ее построения, а также расширения возможностей ее составных частей (сегментов) в зависимости от условий функционирования АСЗИ и требований о ЗИ;
- ЗИ должна обеспечиваться во всех составных частях (сегментах) АСЗИ, используемых в обработке защищаемой информации;
- входящие в состав АСЗИ средства ЗИ и контроля эффективности ЗИ не должны препятствовать нормальному функционированию АСЗИ;

- программное обеспечение системы ЗИ должно быть совместимым с программным обеспечением других составных частей (сегментов) АСЗИ и не должно снижать требуемый уровень защищенности информации в АСЗИ;

- программно-технические средства, используемые для построения системы ЗИ, должны быть совместимы между собой (корректно работать совместно) и не должны снижать уровень защищенности информации в АСЗИ.

ЗИ о создаваемой АСЗИ является составной частью работ по их созданию и осуществляется во всех организациях, участвующих в процессе создания (модернизации) этих систем.

Обеспечение ЗИ в АСЗИ достигается заданием, реализацией и контролем выполнения требований о защите информации:

- к процессу хранения, передачи и обработки защищаемой в АСЗИ информации;

- к системе ЗИ;

- к взаимодействию АСЗИ с другими АС;

- к условиям функционирования АСЗИ;

- к содержанию работ по созданию (модернизации) АСЗИ на различных стадиях и этапах ее создания (модернизации);

- к организациям (должностным лицам), участвующим в создании (модернизации) и эксплуатации АСЗИ;

- к документации на АСЗИ;

- к АСЗИ в целом.

АСЗИ должны создаваться в соответствии с ТЗ, являющимся основным документом, на основании которого выполняются работы, необходимые для создания (модернизации) АСЗИ в целом и ее системы ЗИ, и осуществляется приемка этих работ заказчиком.

Процесс построения АСЗИ должен представлять собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания АСЗИ, соответствующей заданным к ней требованиям.

3.2. Содержание работ по созданию АС в защищенном исполнении

Стадии и этапы работ по созданию АСЗИ устанавливаются в ТЗ на АСЗИ на основе ГОСТ 34.601 с учетом положений настоящего стандарта.

Состав и содержание работ могут уточняться в соответствии с требованиями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов по ЗИ, а также в соответствии с требованиями заказчика АСЗИ.

В ТЗ на создание АСЗИ для реализуемых в соответствии с ним стадий и этапов ее создания должны включаться требования к системе ЗИ АСЗИ, а также требования по ЗИ о создаваемой АСЗИ в соответствии с настоящим стандартом, нормативными правовыми актами и методическими документами уполномоченных федеральных органов исполнительной власти и другими национальными стандартами.

Мероприятия по ЗИ должны проводиться на всех стадиях и этапах создания АСЗИ с учетом применимых (исходя из предназначения АСЗИ) требований нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов в области ЗИ.

Для АСЗИ, создаваемой на базе действующей АС, разрабатывают ТЗ на создание системы ЗИ или дополнение к основному ТЗ на АС, в которое включают требования к системе ЗИ, а также к той части АС, которая подлежит доработке (модернизации) в связи с включением в состав АС системы ЗИ.

Разработка, утверждение и согласование ТЗ или дополнения к ТЗ на модернизируемую АС осуществляется в порядке, установленном ГОСТ 34.602.

Документация на АСЗИ должна разрабатываться с учетом требований ГОСТ 34.201 и [5], а также требований нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов по ЗИ.

Работы по созданию АСЗИ должны проводиться в соответствии с требованиями нормативных правовых актов и методических документов уполномоченного федерального органа исполнительной власти, настоящего стандарта и других национальных стандартов по ЗИ. Дополнительно при необходимости могут учитываться требования национальных стандартов, приведенных в приложении А.

Для создания АСЗИ могут применяться как серийно выпускаемые, так и специальные (разрабатываемые в ходе создания АСЗИ) ТС и ПС обработки информации, а также технические, программные, программно-аппаратные, криптографические СЗИ и средства контроля эффективности ЗИ. Указанные средства должны иметь сертификаты соответствия, полученные в соответствующих системах сертификации по требованиям безопасности информации [6, 7]. Специальные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации АСЗИ организациями (учреждениями), имеющими лицензии уполномоченных федеральных органов исполнительной власти на соответствующие виды деятельности.

Работы по созданию и эксплуатации АСЗИ с использованием криптографических средств организуются в соответствии с положениями нормативных актов Российской Федерации, определяющих порядок разработки, изготовления, сопровождения и эксплуатации криптографических средств.

Организационно-методическое руководство работами по созданию, изготовлению, обеспечению и эксплуатации средств криптографической ЗИ, по сертификации этих средств осуществляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

Перед вводом в эксплуатацию комплексов ТС АСЗИ (в случае отсутствия документа, подтверждающего уже проведенные исследования) и периодически в процессе их эксплуатации проводятся исследования по криптографической ЗИ в составе комплексов ТС АСЗИ организациями, имеющими лицензию на этот вид работ в соответствии с [4].

Порядок эксплуатации АСЗИ с использованием криптографических средств регламентируется законодательством Российской Федерации и нормативными правовыми актами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности.

Организация надлежащего исполнения правил эксплуатации средств криптографической ЗИ (в том числе во время приемочных испытаний) возлагается на руководство организаций, эксплуатирующих данные средства.

Контроль выполнения требований инструкций по эксплуатации средств криптографической ЗИ возлагается на специальные подразделения (штатных специалистов) по ЗИ на предприятии (организации), эксплуатирующем данные средства.

Виды испытаний АСЗИ и общие требования к их проведению определяются ГОСТ 34.603, а также нормативными правовыми актами и методическими документами уполномоченного федерального органа исполнительной власти и национальными стандартами по ЗИ.

Испытания АСЗИ на соответствие требованиям безопасности информации от ее утечки по техническим каналам, несанкционированного доступа к ней, от несанкционированных и непреднамеренных воздействий на информацию, в том числе по криптографической и антивирусной защите, по обнаружению вторжений (атак) и др. осуществляются в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов.

В случаях, установленных федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, нормативными правовыми актами уполномоченных федеральных органов

исполнительной власти, для подтверждения соответствия системы ЗИ АСЗИ в реальных условиях эксплуатации требованиям безопасности информации осуществляется аттестация АСЗИ на соответствие требованиям безопасности информации.

Аттестация АСЗИ проводится до ввода АСЗИ в постоянную эксплуатацию в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов.

3.3. Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении

3.1.1 Защита информации в АСЗИ обеспечивается системой ЗИ АСЗИ. Создание системы ЗИ АСЗИ обеспечивается следующим комплексом работ:

- формирование требований к системе ЗИ АСЗИ;
- разработка (проектирование) системы ЗИ АСЗИ;
- внедрение системы ЗИ АСЗИ;
- аттестация АСЗИ на соответствие требованиям безопасности информации и ввод ее в действие;
- сопровождение системы ЗИ в ходе эксплуатации АСЗИ.

Формирование требований к системе ЗИ АСЗИ организуется заказчиком и осуществляется разработчиком на основе требований по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, несанкционированных и непреднамеренных воздействий на информацию, в том числе требований по криптографической и антивирусной защите, по обнаружению вторжений (атак), обеспечению устойчивости и непрерывности функционирования АСЗИ и др., закрепленных в нормативных правовых актах уполномоченных федеральных органов исполнительной власти и национальных стандартах в области ЗИ, с учетом целей и задач АСЗИ, свойственных ей угроз безопасности информации и возможных последствий реализации этих угроз.

Формирование требований к системе ЗИ АСЗИ осуществляется на следующих стадиях создания АСЗИ, определенных ГОСТ 34.601:

- "Формирование требований к АС";
- "Разработка концепции АС";
- "Техническое задание".

Требования к системе ЗИ АСЗИ уточняются на последующих стадиях создания АСЗИ, с конкретизацией требований к ее построению, используемым информационным технологиям, методам и программно-аппаратным средствам организации сетевого взаимодействия, в том числе с

другими системами, к процессу обработки защищаемой информации, условиям функционирования АСЗИ.

На стадии "Формирование требований к АС" в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

На этапе "Обследование объекта и обоснование необходимости создания АС" проводят:

- анализ данных о назначении, функциях, условиях функционирования создаваемой (модернизируемой) АСЗИ и характере обрабатываемой информации;
- определение перечня информации, подлежащей защите;
- определение актуальных угроз безопасности информации, связанных с НСД к защищаемой информации, с утечкой информации по техническим каналам и с несанкционированным воздействием на информацию;
- разработку модели угроз безопасности информации применительно к конкретным вариантам функционирования АСЗИ;
- оценку (технико-экономической и т.п.) целесообразности создания АС в защищенном исполнении.

На этапе "Формирование требований пользователя к АС" проводят:

а) подготовку исходных данных для формирования требований в части системы ЗИ к создаваемой (модернизируемой) АСЗИ (исходя из её предназначения и условий использования), включая:

- определение порядка обработки информации в АСЗИ в целом и в отдельных компонентах;
- оценку степени участия персонала в обработке (обсуждении, передаче, хранении) защищаемой в АСЗИ информации;
- определение требуемого класса (уровня) защищенности АСЗИ от НСД;
- выбор целесообразных (исходя из экономических, научно-технических, временных и других ограничений, а также технологии обработки информации) способов ЗИ и контроля состояния ЗИ в АСЗИ;
- обоснование архитектуры и конфигурации системы ЗИ АСЗИ и ее отдельных составных частей, физических, функциональных и технологических связей как внутри АСЗИ, так и с другими взаимодействующими системами;
- выбор ТС, которые могут быть использованы при разработке системы ЗИ АСЗИ;
- оценку возможности создания АСЗИ, исходя из ресурсных ограничений;

б) формирование требований к системе ЗИ создаваемой (модернизируемой) АСЗИ в части требований о защите информации.

На этапе "Оформление отчета о выполненной работе и заявки на разработку АС (ТТЗ)" проводят:

- систематизацию результатов, полученных на предыдущих этапах;
- формирование разделов отчета о выполненных работах на данной стадии в части создания системы ЗИ для создаваемой (модернизируемой) АСЗИ;
- оформление заявки на разработку системы ЗИ (ТЗ или дополнения к ТЗ) или другого заменяющего ее документа с аналогичным содержанием (в случае разработки отдельного ТЗ на систему ЗИ АСЗИ).

На стадии "Разработка концепции АС" в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

На этапе "Изучение объекта" проводят:

- определение путей и оценку возможности реализации требований, предъявляемых к системе ЗИ создаваемой (модернизируемой) АСЗИ;
- обоснование необходимости привлечения организаций, имеющих необходимые лицензии, для создания системы ЗИ создаваемой (модернизируемой) АСЗИ;
- оценку ориентировочных сроков создания системы ЗИ АСЗИ;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение системы ЗИ создаваемой (модернизируемой) АСЗИ;
- обоснование целесообразности проведения НИР (составной части НИР), определение основных вопросов, подлежащих исследованию в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ;
- разработку ТТЗ на НИР (при необходимости).

На этапе "Проведение необходимых научно-исследовательских работ" проводят:

- анализ требований к назначению, структуре и конфигурации создаваемой (модернизируемой) АСЗИ;
- уточнение режимов обработки информации в АСЗИ в целом и в отдельных компонентах;
- анализ возможных уязвимостей и обоснование актуальных угроз безопасности информации и перечня мероприятий по их блокированию (нейтрализации);
- уточнение требований о ЗИ в АСЗИ;
- уточнение требований к архитектуре и конфигурации системы ЗИ АСЗИ;
- уточнение требований к составу и характеристикам основных и вспомогательных ПС и ТС, которые могут быть использованы при разработке системы ЗИ АСЗИ, режимам их работы;

- обоснование перечня сертифицированных средств ЗИ, использование которых возможно в составе системы ЗИ создаваемой (модернизируемой) АСЗИ;

- уточнение оценки материальных, трудовых и финансовых затрат на создание системы ЗИ создаваемой (модернизируемой) АСЗИ;

- оформление и утверждение отчета о НИР.

На этапе "Разработка вариантов концепции АС и выбор варианта концепции АС, удовлетворяющего требованиям пользователя" проводят:

- разработку альтернативных вариантов концепции создаваемой системы ЗИ и планов их реализации;

- оценку необходимых ресурсов на реализацию каждого варианта и обеспечение функционирования системы ЗИ;

- оценку эффектов, преимуществ и недостатков от реализации каждого варианта;

- выбор варианта концепции системы ЗИ АСЗИ.

На этапе "Оформление отчета о выполненной работе" разрабатывается самостоятельный отчет о работах, выполненных на стадии "Разработка концепции АС" в части системы ЗИ или раздел в основной отчет о работах, выполненных в интересах создания (модернизации) АСЗИ в целом.

На стадии "Техническое задание" в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

На этапе "Разработка и утверждение технического задания на создание АС" проводят разработку, оформление, согласование и утверждение ТЗ на АСЗИ в целом и, при необходимости, ТЗ на систему ЗИ.

ТЗ (раздел ТЗ, дополнение к ТЗ) на систему ЗИ должно разрабатываться в соответствии с требованиями ГОСТ 34.602.

3.1.2 Разработка (проектирование) системы ЗИ АСЗИ включает:

- разработку проектных решений по системе ЗИ АСЗИ;

- разработку документации на систему ЗИ АСЗИ;

- тестирование системы ЗИ АСЗИ.

3.1.3 Разработку системы ЗИ АСЗИ организует заказчик, проводит разработчик в соответствии с ТЗ на создание системы ЗИ АСЗИ на следующих стадиях создания АСЗИ, определенных ГОСТ 34.601:

- Эскизный проект;

- Технический проект;

- Рабочая документация.

На стадии "Эскизный проект" в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

На этапе "Разработка предварительных проектных решений по системе и ее частям" проводят:

- определение субъектов доступа (пользователей, процессов и иных субъектов доступа) и объектов доступа (устройств, объектов файловой системы, запускаемых и исполняемых модулей, объектов системы управления базами данных, объектов, создаваемых прикладным программным обеспечением, иных объектов доступа);

- уточнение исходных данных, касающихся технических, информационных, программных и организационных аспектов создания и функционирования системы ЗИ АСЗИ и АСЗИ в целом;

- определение функций системы ЗИ создаваемой (модернизируемой) АСЗИ, состава комплексов задач и отдельных задач, решаемых подсистемой ЗИ;

- проработку и рассмотрение вариантов построения системы ЗИ с учетом результатов ранее проведенных исследований и новейших достижений науки и техники, в том числе по зарубежным аналогам, определение общих требований к системе ЗИ (ее структура, состав (число) и места размещения составных частей системы ЗИ);

- определение функций и параметров ТС и ПС системы ЗИ, особенностей их реализации в интересах блокирования (нейтрализации) угроз безопасности информации в АСЗИ;

- определение состава организационных мер ЗИ, ТС и ПС системы ЗИ, выбор сертифицированных СЗИ с учетом их совместимости с основными ТС и ПС создаваемой (модернизируемой) АСЗИ;

- обоснование номенклатуры СЗИ, специального технологического оборудования, средств контроля и измерений, подлежащих разработке в ходе создания АСЗИ.

На этапе "Разработка документации на АС и ее части" проводят разработку, оформление, согласование и утверждение документации в объеме, необходимом для описания полной совокупности принятых предварительных проектных решений и достаточном для дальнейшего выполнения работ по созданию системы ЗИ. Виды документов - по ГОСТ 34.201.

На стадии "Технический проект" в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ выполняют следующие работы.

На этапе "Разработка проектных решений по системе и ее частям" обеспечивают:

- разработку общих решений по системе ЗИ, по ее функциональной структуре, ТС и ПС системы ЗИ, алгоритмам функционирования системы ЗИ, функциям персонала, обслуживающего систему ЗИ;

- разработку алгоритмов решения задач ЗИ, параметров настройки ТС и ПС, обеспечивающих реализацию функциональных возможностей системы ЗИ;

- разработку макетов составных частей системы ЗИ (при необходимости).

На этапе "Разработка документации на АС и ее части" проводят разработку, оформление, согласование и утверждение технической документации на систему ЗИ. Виды документов - по ГОСТ 34.201.

На этапе "Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку" проводят:

- подготовку и оформление документов на поставку ТС и ПС для комплектования системы ЗИ создаваемой (модернизируемой) АСЗИ;

- определение технических требований и составление ТЗ на разработку специальных СЗИ, специального технологического оборудования, средств контроля и измерений, не изготавливаемых серийно.

На этапе "Разработка заданий на проектирование в смежных частях проекта объекта информатизации" осуществляют разработку, оформление, согласование и утверждение заданий на проектирование помещений для АСЗИ с учетом требований о ЗИ.

На стадии "Рабочая документация" в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ проводят следующие работы.

На этапе "Разработка рабочей документации на систему и ее части" осуществляют разработку рабочей документации на систему ЗИ, содержащей все необходимые и достаточные сведения для обеспечения выполнения работ по вводу системы ЗИ АСЗИ в действие и ее эксплуатации, в том числе для поддержания уровня эксплуатационных характеристик (качества) системы ЗИ в соответствии с принятыми проектными решениями, ее оформление, согласование и утверждение, а также разработку программы и методик испытаний системы ЗИ. Виды документов - по ГОСТ 34.201.

На этапе "Разработка и адаптация программ" проводят:

- разработку ПС для СЗИ, адаптацию и/или привязку приобретаемых ПС, тестирование ПС системы ЗИ АСЗИ;

- разработку и испытания СЗИ, технологического оборудования, средств контроля и измерений системы ЗИ АСЗИ;

- сертификацию разрабатываемых ПС и СЗИ системы ЗИ АСЗИ по требованиям безопасности информации;

- разработку документации на ПС и СЗИ системы ЗИ АСЗИ;

- тестирование ПС системы ЗИ АСЗИ.

При тестировании ПС системы ЗИ АСЗИ:

- проверяют работоспособность и совместимость ПС системы ЗИ с информационными технологиями и ТС обработки информации;

- проверяют выполнение ПС системы ЗИ требований к системе ЗИ АСЗИ;

- корректируют документацию на систему ЗИ АСЗИ (при необходимости).

Внедрение системы ЗИ АСЗИ включает:

- установку и настройку СЗИ;
- разработку организационно-распорядительных документов, определяющих мероприятия по ЗИ в ходе эксплуатации АСЗИ;
- предварительные испытания системы ЗИ АСЗИ;
- опытную эксплуатацию и доработку системы ЗИ АСЗИ;
- приемочные испытания системы ЗИ АСЗИ;
- аттестацию АСЗИ на соответствие требованиям безопасности информации.

Внедрение системы ЗИ АСЗИ организует заказчик, проводит разработчик в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информациии рабочей документацией на систему ЗИ АСЗИ на стадии "Ввод в действие", определенной ГОСТ 34.601.

На стадии "Ввод в действие" в интересах внедрения системы ЗИ создаваемой (модернизируемой) АСЗИ проводят следующие работы.

На этапе "Подготовка объекта к вводу АС в действие" проводят работы по реализации:

- проектных решений по организационной структуре системы ЗИ создаваемой (модернизируемой) АСЗИ и АСЗИ в целом;
- организационных мер, обеспечивающих эффективное использование системы ЗИ.

На этапе "Подготовка персонала" проводят:

- обучение персонала АСЗИ и проверку его способности обеспечивать функционирование системы ЗИ и АСЗИ в целом;
- проверку и подготовку специалистов структурного подразделения или должностного лица (работника), ответственных за ЗИ в АСЗИ.

На этапе "Комплектация АС поставляемыми изделиями (программными и техническими средствами, программно-техническими комплексами, информационными изделиями)":

- обеспечивают получение комплектующих изделий системы ЗИ серийного и единичного производства, материалов и монтажных изделий;
- проводят входной контроль качества комплектующих изделий системы ЗИ, проверку наличия документов по сертификации;
- проводят специальные исследования и специальные проверки закупленных средств.

На этапе "Строительно-монтажные работы" осуществляют:

- надзор за выполнением строительными организациями требований ЗИ;

- проверку реализации требований о ЗИ при приемке монтажных работ (в случае необходимости проводят соответствующие испытания).

На этапе "Пусконаладочные работы" осуществляют:

- автономную наладку ТС и ПС системы ЗИ;
- комплексную наладку всех СЗИ системы ЗИ.

На этапе "Проведение предварительных испытаний" осуществляют:

- испытания системы ЗИ на работоспособность и соответствие техническому заданию в соответствии с программой и методикой предварительных испытаний;
- устранение недостатков, выявленных в процессе испытаний, и внесение изменений в документацию на систему ЗИ создаваемой (модернизируемой) АСЗИ, в том числе эксплуатационную, в соответствии с протоколом испытаний;
- принятие решения о возможности опытной эксплуатации системы ЗИ АСЗИ.

На этапе "Проведение опытной эксплуатации" проводят:

- проверку функционирования системы ЗИ в составе АСЗИ, в том числе реализованных мер ЗИ;
- анализ выявленных в ходе опытной эксплуатации системы ЗИ уязвимостей АСЗИ, доработку, наладку системы ЗИ;
- проверку готовности пользователей и администраторов к эксплуатации системы ЗИ АСЗИ;
- оформление акта о завершении опытной эксплуатации системы ЗИ АСЗИ.

На этапе "Проведение приемочных испытаний" проводят:

- испытания системы ЗИ АСЗИ на соответствие ТЗ на систему ЗИ в соответствии с программой и методиками приемочных испытаний АСЗИ;
- анализ результатов испытаний системы ЗИ АСЗИ и устранение недостатков, выявленных при испытаниях;
- оформление разделов акта о приемке АСЗИ в постоянную эксплуатацию (в части системы ЗИ АСЗИ).

Аттестацию АСЗИ на соответствие требованиям безопасности информации организует заказчик, проводит организация, имеющая лицензию на данный вид деятельности, до ввода АСЗИ в эксплуатацию, с использованием информационных ресурсов, подлежащих защите, и содержит оценку соответствия ее системы ЗИ требованиям безопасности информации в реальных условиях эксплуатации, проводимую в соответствии с требованиями нормативных правовых актов и методических документов уполномоченного федерального органа исполнительной власти, а также национальных стандартов в области защиты информации.

Сопровождение системы ЗИ в ходе эксплуатации АСЗИ организует заказчик (оператор), проводит разработчик в соответствии с проектными решениями, рабочей документацией на систему ЗИ АСЗИ, организационно-распорядительными документами по ЗИ. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ заключается в выполнении работ относительно системы ЗИ АСЗИ в соответствии с гарантийными обязательствами и по послегарантийному обслуживанию, которые осуществляются на стадии "Сопровождение АС", определенной ГОСТ 34.601.

На стадии "Сопровождение АС" проводят следующие работы.

На этапе "Выполнение работ в соответствии с гарантийными обязательствами" осуществляют работы по:

- устранению недостатков системы ЗИ, выявленных в процессе эксплуатации АСЗИ, и последующему контролю за стабильностью характеристик системы ЗИ АСЗИ, влияющих на эффективность ЗИ в течение установленных гарантийных сроков;
- внесению изменений в документацию на систему ЗИ и, при необходимости, в документацию на АСЗИ в целом.

На этапе "Послегарантийное обслуживание" осуществляют работы по:

- мониторингу качества функционирования системы ЗИ АСЗИ;
- установлению причин невыполнения требований о ЗИ в процессе функционирования АСЗИ;
- устранению недостатков в системе ЗИ и контролю за стабильностью ее характеристик, влияющих на эффективность ЗИ;
- внесению изменений в документацию на систему ЗИ и, при необходимости, в документацию на АСЗИ в целом.

Глава 4. ХАРАКТЕРИСТИКА ПОДСИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

4.1. Базовые подсистемы защиты информации в составе объекта информатизации.

Защита от несанкционированного доступа в локальных вычислительных сетях (ЛВС) и отдельных компьютеров, а также в открытых сетях, например, в сети Internet, требует качественного решения трех базовых задач:

- Защиты информации на уровне отдельных компьютеров и ЛВС.
- Защиты подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды.
- Защиты информации в процессе передачи по открытым каналам связи (через Internet).

Для этих целей проектируются и создаются программно-аппаратные средства защиты информации от несанкционированного доступа, которые в общем случае можно разделить на группы, как показано на рисунке 4.1:

- Средства защиты информации на уровне отдельных компьютеров и ЛВС.
- Средства защиты информации отдельных компьютеров и ЛВС со стороны внешней среды.
- Средства защиты информации на уровне сети Интернет.

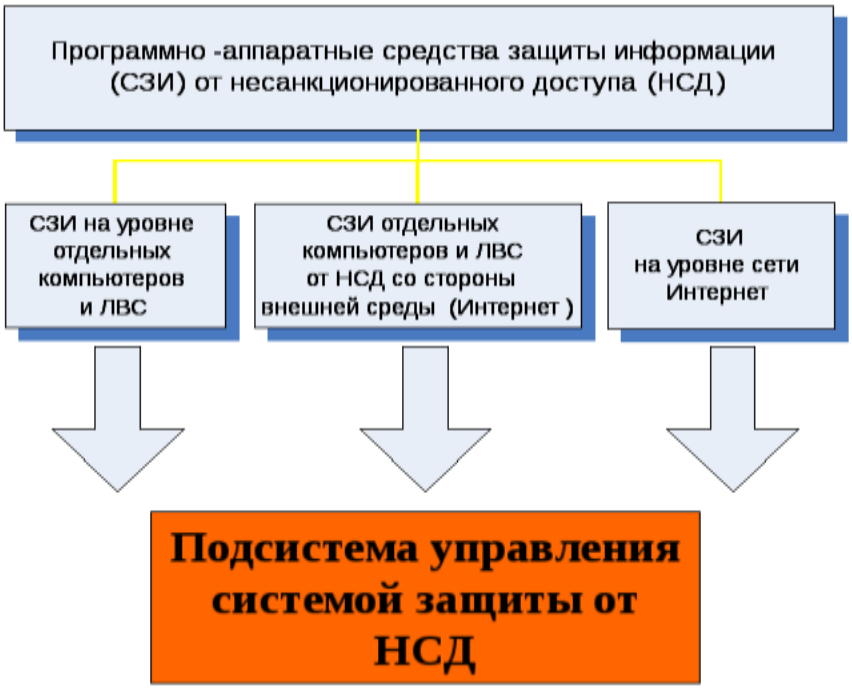

Рисунок 4.1 – Классификация ПАС защиты информации от НСД.

Все программно-аппаратные средства защиты информации от несанкционированного доступа включают в себя, так называемую подсистему управления системой защиты информации, которая реализуется в рамках системы защиты информации от НСД, условно состоящей из подсистем, как показано на рисунке 4.2:

- Подсистемы управления доступом;
- Подсистемы регистрации и учета;
- Криптографической подсистемы;
- Подсистемы обеспечения целостности,
- Подсистемы антивирусной защиты,
- Подсистемы управления системой защиты информации, предназначенной для эффективного управления вышеназванных подсистем.

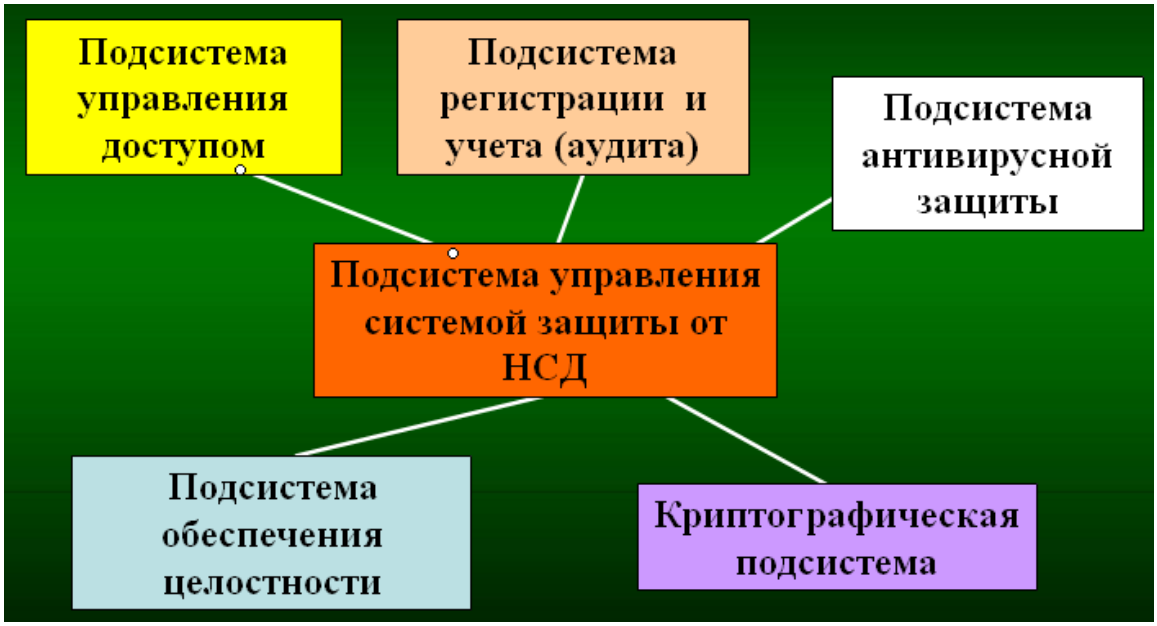

Рисунок 4.2 – Состав системы защиты информации от НСД

Выделяются следующие основные группы механизмов защиты:

- механизмы управления доступом;
- механизмы регистрации и учета;
- механизмы криптографической защиты;
- механизмы контроля целостности.

Отметим, что первая группа “Подсистема управления доступом” является основополагающей для реализации защиты от НСД, т.к. именно механизмы защиты данной группы призваны непосредственно противодействовать несанкционированному доступу к компьютерной информации.

Остальные же группы механизмов реализуются в предположении, что механизмы защиты первой группы могут быть преодолены злоумышленником.

В частности они могут использоваться:

- для контроля действий пользователя — группа “Подсистема регистрации и учета”;
- для противодействия возможности прочтения похищенной информации (например, значений паролей и данных) — группа “Криптографическая подсистема”;
- для контроля осуществленных злоумышленником изменений защищаемых объектов (исполняемых файлов и файлов данных) при осуществлении к ним НСД и для восстановления защищаемой информации из резервных копий – группа “Подсистема обеспечения целостности”.

Кроме того, эти группы механизмов могут использоваться для проведения расследования по факту НСД.

Подсистема антивирусной защиты является неотъемлемой частью системы защиты СЗИ от НСД. При её правильной настройке значительно уменьшается риск воздействия вредоносных программ.

Но никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам.

В общем случае функциями подсистемы антивирусной защиты являются:

- Предотвращение заражения АРМ пользователя вредоносными программами;
- Обнаружение вредоносных программ;
- Удаление вредоносной программы из зараженного АРМ пользователя.

4.2. Требования к подсистемам защиты информации

Подсистема управления доступом должна удовлетворять следующим требованиям:

- Идентифицировать и проверять подлинность субъектов доступа при входе в систему. Причем это должно осуществляться по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.
- Идентифицировать терминалы, ЭВМ, узлы компьютерной сети, каналы связи, внешние устройства ЭВМ по их логическим адресам (номерам).
- По именам идентифицировать программы, тома, каталоги, файлы, записи и поля записей.

• Осуществлять контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема регистрации и учета должна:

1) Регистрировать вход (выход) субъектов доступа в систему (из системы), либо регистрировать загрузку и инициализацию операционной системы. При этом в параметрах регистрации указываются:

• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

• результат попытки входа — успешная или неуспешная (при НСД);

• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

• код или пароль, предъявленный при неуспешной попытке.

2) Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

3) Регистрировать выдачу печатных (графических) документов на твердую копию. При этом в параметрах регистрации указываются:

• дата и время выдачи (обращения к подсистеме вывода);

• краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

• спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

• идентификатор субъекта доступа, запросившего документ.

4) Регистрировать запуск (завершение) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.

При этом в параметрах регистрации указывается:

• дата и время запуска;

• имя (идентификатор) программы (процесса, задания);

• идентификатор субъекта доступа, запросившего программу (процесс, задание);

• результат запуска (успешный, неуспешный — несанкционированный).

5) Регистрировать попытки доступа программных средств (программ,

процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указывается:

• дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная — несанкционированная);

• идентификатор субъекта доступа;

• спецификация защищаемого файла.

6) Регистрировать попытки доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ,

узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. При этом в параметрах регистрации указывается:

• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная, несанкционированная;

• идентификатор субъекта доступа;

• спецификация защищаемого объекта [логическое имя (номер)].

7) Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

8) Регистрировать выдачу (приемку) защищаемых носителей.

9) Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. При этом очистка должна производиться однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Подсистема обеспечения целостности должна:

1) Обеспечивать целостность программных средств системы защиты информации от НСД (СЗИ НСД), обрабатываемой информации, а также неизменность программной среды. При этом:

• целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

• целостность программной среды обеспечивается использованием трансляторов с языка высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

2) Осуществлять физическую охрану СВТ (устройств и носителей информации). При этом должны предусматриваться контроль доступа в помещение АС посторонних лиц, а также наличие надежных препятствий для несанкционированного проникновения в помещение АС и хранилище носителей информации. Особенно в нерабочее время.

3) Проводить периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест программ, имитирующих попытки НСД.

4) Иметь в наличии средства восстановления СЗИ НСД. При этом предусматривается ведение двух копий программных средств СЗИ НСД, а также их периодическое обновление и контроль работоспособности.

К базовым функциям подсистемы управления доступом относятся

- Идентификация и аутентификация (проверка подлинности) пользователей;

- Управление доступом пользователей к защищаемым ресурсам;
- Создание замкнутой рабочей среды для пользователей.

Идентификацию и *аутентификацию* можно считать основой программно-технических средств безопасности. *Идентификация* и *аутентификация*– это первая линия обороны, "проходная" информационного пространства организации.

Идентификатор– уникальный признак субъекта или объекта доступа.

Идентификация– присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация– проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством ***аутентификации*** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "*аутентификация*" иногда используют словосочетание "проверка подлинности".

Субъект может подтвердить свою подлинность, предъявив, по крайней мере, одну из следующих сущностей:

- нечто, что он знает (пароль, личный *идентификационный* номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку, смарт-карта или бейдж или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, снимок сетчатки глаза и т.п., то есть свои биометрические характеристики).

Таким образом, методами аутентификации пользователей являются:

- Парольная аутентификация;
- Маркеры аутентификации;
- Биометрическая аутентификация.

Главное достоинство ***парольной аутентификации*** – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности по следующим причинам:

Альтернативой паролям являются ***смарт-карты (маркеры аутентификации) и биометрия***. Однако развертывание таких систем связано с дополнительными расходами.

Для установления личности используются ***смарт-карты***, и таким образом уменьшается риск угадывания пароля. Однако если смарт-карта украдена, и это - единственная форма установления подлинности, то похититель сможет замаскироваться под легального пользователя компьютерной системы. Смарт-карты не смогут предотвратить атаку с использованием уязвимых мест, поскольку они рассчитаны на правильный вход пользователя в систему.

Биометрические системы - механизм аутентификации, значительно уменьшающий вероятность угадывания пароля.

Существует множество биометрических сканеров для верификации следующего:

- отпечатков пальцев;
- сетчатки/радужной оболочки;
- отпечатков ладоней;
- конфигурации руки;
- конфигурации лица;
- голоса.

Биометрия представляет собой совокупность автоматизированных методов *идентификации* и/или *аутентификации* людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности **отпечатков пальцев, сетчатки** и **роговицы** глаз, **геометрия руки и лица** и т.п. К поведенческим характеристикам относятся **динамика подписи**, стиль **работы с клавиатурой**. На стыке физиологии и поведения находятся анализ особенностей **голоса** и **распознавание речи**. Каждый подход предполагает использование определенного устройства для идентификации человеческих характеристик. Обычно эти устройства довольно сложны, чтобы исключить попытки обмана. Например, при снятии отпечатков пальцев несколько раз проверяются температура и пульс. При использовании биометрии возникает множество проблем, включая стоимость развертывания считывающих устройств и нежелание сотрудников их использовать.

Управление доступом пользователей к защищаемым ресурсам.

После идентификации и аутентификации пользователя при функционировании компьютерной системы система защиты должна постоянно контролировать правомерность его доступа компьютерным ресурсам. Для этого при попытке доступа любого пользователя к какому-либо ресурсу система защиты должна проанализировать полномочия этого пользователя, находящиеся в своей базе данных, и разрешить доступ только в случае соответствия запроса на доступ пользовательским полномочиям.

Процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам называют разграничением

доступа или управлением доступом, а подсистему защиты, выполняющую эти функции - подсистемой разграничения доступа или управления доступом к компьютерным ресурсам, что показано на рисунке 4.3.

Рисунок 4.3 – Управление доступом пользователей к защищаемым ресурсам

Средства разграничения доступа позволяют специфицировать и контролировать действия, которые субъекты - пользователи и процессы могут выполнять над объектами - информацией и другими компьютерными ресурсами. Логическое управление доступом, реализуемое после идентификации и аутентификации пользователей, - это один из основных способов, призванный обеспечить конфиденциальность, целостность и подлинность информационных объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей.

Подсистема разграничения доступа к компьютерным ресурсам реализует концепцию единого диспетчера доступа, являющегося посредником при всех обращениях субъектов к объектам.

Диспетчер доступа должен выполнять следующие функции:

- проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты (правил разграничения доступа);
- при необходимости регистрировать факт доступа и его параметры в системном журнале регистрации.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой **произвольного (или дискреционного) управления доступом**;
- атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа **принудительного (мандатного) управления доступом.**

Если при попытке доступа пользователя к компьютерным ресурсам подсистема разграничения определяет факт несоответствия запроса на доступ пользовательским полномочиям, то доступ блокируется, и могут предусматриваться следующие санкции за попытку несанкционированного доступа:

- предупреждение пользователя;
- отключение пользователя от вычислительной системы на некоторое время;
- полное отключение пользователя от системы до проведения административной проверки;
- подача сигнала службе безопасности о попытке несанкционированного доступа с отключением пользователя от системы;
- регистрация попытки несанкционированного доступа.

Основными методами разграничения доступа пользователей являются:

- произвольное (дискреционного) разграничение;
- принудительное (мандатного) разграничение. Это показано на рисунке 4.4.

Рисунок 4.4 – Методы разграничения доступа пользователей

Произвольное или, как его еще называют, дискреционное управление доступом - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту. Владельцем объекта, как правило, считается пользователь, создавший данный объект.

При принудительном разграничении доступа компьютерные ресурсы разделяются на группы в соответствии с уровнями секретности и категориями информации, к которым они относятся. В качестве уровней секретности могут быть выделены следующие:

- «несекретно»;
- «для служебного использования»;
- «секретно»;
- «совершенно секретно».

Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. В военной области каждая категория может соответствовать определенному виду вооружений. Например, все тактико-технические данные о средствах вооружения могут быть разделены по типам этих средств - данные о наземных, морских, а также воздушных средствах вооружения. Механизм категорий позволяет разделить информацию по видам, что способствует лучшей защищенности.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта, называемая еще мандатом, описывает его благонадежность и задает:

- максимальный уровень секретности информации, доступ к которой ему разрешен;
- категории информации, к которой он допущен.

Метка объекта определяет степень закрытости и категории содержащейся в нем информации.

Создание замкнутой рабочей среды для пользователей.

Немаловажную роль играет создание для каждого пользователя ограниченной виртуальной среды, скрывающей запрещенные ресурсы и не предоставляющей средства доступа к этим ресурсам. С этой целью для рабочих станций достаточно создать замкнутое интерфейсное окружения, при котором пользователь будет иметь возможность доступа только к тем программам и элементам интерфейса, которые разрешены администратором. В этом случае можно заблокировать доступ к панели управления, системным дискам рабочих станций и установить список только разрешенных программ. Данные возможности на основе использования правил системной политики предоставляют встроенные средства ПО.

К базовым функциям подсистемы регистрации и учёта, как показано на рисунке 4.5, относятся:

- Регистрация и учёт действий пользователей;
- Гарантированное уничтожение остаточных данных;
- Учёт машинных носителей информации.

Рисунок 4.5 – Базовые функции подсистемы регистрации и учёта

Регистрация и учет действий пользователей представляют собой совокупность средств, используемых для регулярного сбора, фиксации и выдачи по запросам сведений обо всех обращениях к защищаемым компьютерным ресурсам, а также доступе в компьютерную систему и выходе из нее, что отражает рисунок 4.6.

Рисунок 4.6 – Регистрация и учет действий пользователей

Регистрация преследует следующие главные цели:

- обеспечение подотчетности пользователей и администраторов (контроль действий пользователей путем удаленного доступа к локаль-

ным журналам регистрации и получения изображений с экранов рабочих станций;);

- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Для защиты от сбоев и отказов регистрируются также сведения обо всех действиях пользователей и программ по модификации данных на внешних информационных носителях.

Говоря о регистрации, часто различают такие понятия, как протоколирование и аудит. Протоколирование предполагает сбор и накопление информации о событиях, происходящих в компьютерной системе, а аудит - анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Основной формой регистрации является программное ведение специальных регистрационных журналов, представляющих собой файлы на внешних носителях информации.

При протоколировании сведений по обращению к компьютерной системе и ее ресурсам рекомендуется фиксировать:

- время поступления запроса;
- идентификатор пользователя, от имени которого выдан запрос;
- идентификатор компьютера (терминала), с которого поступил запрос;
- содержание сообщения в составе запроса;
- реквизиты защиты (полномочия пользователей, пароли, коды, ключи и др.), используемые при выполнении запроса;
- время окончания использования ресурса.

Имея такие сведения в любой момент можно получить статистические данные относительно компьютеров (терминалов), пользователей и программ, запрашивающих доступ, а также сведения о результатах выполнения запросов и характере использования запрашиваемых ресурсов.

При протоколировании всех действий пользователей и программ по модификации данных на внешних информационных носителях следует фиксировать все изменения как системной, так и несистемной информации между непротиворечивыми состояниями файловой структуры и содержимого файлов. Это обеспечивает поддержание логической целостности данных на основе возможности их восстановления при возникновении сбоев и отказов программно-аппаратных средств вычислительной системы.

Гарантированное уничтожение секретной информации.

Если важный документ просто выбрасывается в мусорную корзину, то он становится добычей для злоумышленников. Секретные документы

нужно разрезать на мелкие части. Канцелярская бумагорезательная машина дает дополнительный уровень защиты, измельчая документ в продольном и поперечном направлении. Вряд ли такой документ можно восстановить!

Информацию в компьютерных системах можно восстановить после удаления, если она удалена неправильно (рисунок 4.7). Для гарантированного уничтожения остаточной информации должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация.

Рисунок 4.7 – Гарантированное уничтожение остаточных данных

Способы уничтожения информации на жестком диске делятся на три группы:

Программные; Механические; Физические.

Программные. Существуют программы, которые стирают данные с магнитных носителей без возможности их восстановления, например PGP desktop и BCWipe.

Недостатки: низкая надежность уничтожения информации; перезапись информации возможна только на исправном диске.

Достоинства: возможность повторного использования диска; низкая стоимость эксплуатации ПО или спец. средств.

Механические. Это способы, связанные с механическими повреждениями основы, на которую нанесен магнитный слой – физический носитель информации. Заключается в измельчении носителя путем пропуска через измельчающую машину. Проводится вскрытие гермокамеры диска, куда попадает пыль, которая как наждак стирает до стекла поверхность диска.

Термический способ - нагревание носителя до 800-1000 градусов - переход магнитного материала рабочего слоя через точку Кюри. Этот способ рекомендован для уничтожения сведений, составляющих государственную тайну.

Пиротехнический способ – разрушение взрывом.

Химический способ – разрушение химически агрессивной средой.

Радиационный способ – разрушение носителя ионизирующими излучениями.

Физические. Связанные с перестройкой структуры магнитного материала рабочих поверхностей носителя: размагничивание рабочих поверхностей носителей; намагничивание рабочих поверхностей носителей до максимально возможных значений намагниченности.

Помимо имеющихся способов существуют и *алгоритмы гарантированного уничтожения информации:*

- DoD5220 (был принят в 1995г. для использования в армии США);
- алгоритм Брюса Шнайра – считается одним из наиболее эффективных;
- алгоритм Путера Гутмана – в его основе 35 циклов стирания информации;
- ГОСТ Р 50739-95 – для систем 4-6 классов защиты;
- РД Гостехкомиссии для классов 3А, 2А «Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения».

Учёт машинных носителей информации предполагает выполнение следующих действий:

-должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

-учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

-должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.

Подсистема обеспечения (контроля) целостности.

Подсистема предназначена для контроля целостности файлв и секторов жесткого диска, с целью убедиться, что эти файлы и сектора не были модифицированы. Для этого вычисляются контрольные значения проверяемых объектов и сравниваются с эталонными значениями, заранее рассчитанными для каждого из этих объектов.

К базовым функциям подсистемы обеспечения целостности информации, как показано на рисунке 4.8, относятся:

- модуль контроля целостности программного и информационного окружения;
- резервирование и восстановление информации.

Рисунок 4.8 – Базовые функции подсистемы обеспечения целостности информации

Модуль контроля целостности является программным модулем ROMBIOS.

Под контролем (поддержанием) целостности программного и информационного окружения понимается её неизменность (физическая целостность) и непротиворечивость (логическая целостность).

- Эффективность контроля целостности основана на проверке соответствия текущих характеристик информационных объектов их эталонным характеристикам (Рисунок 4.9).

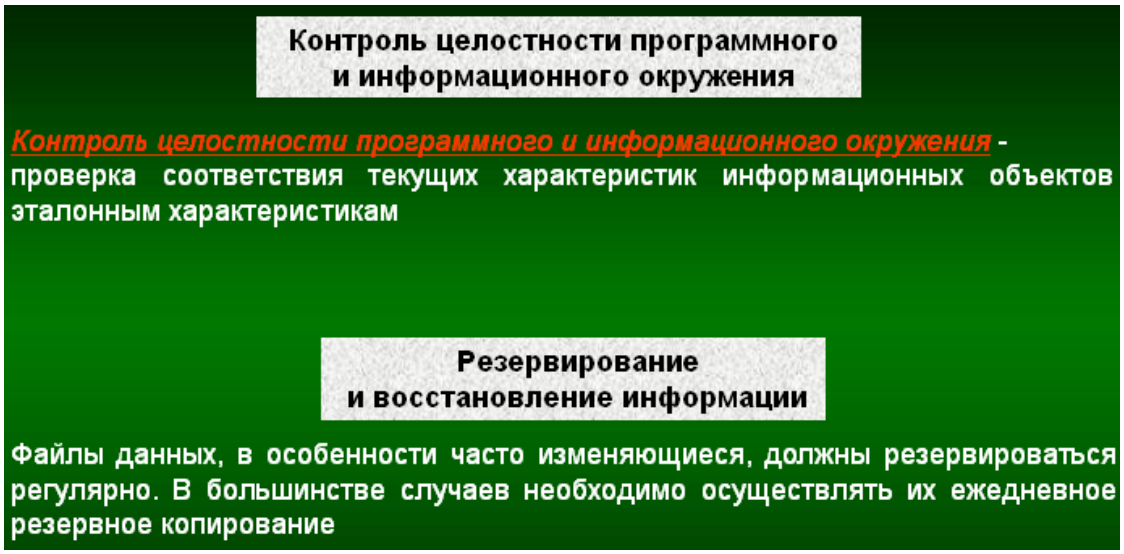

Рисунок 4.9 – а) Контроль целостности программного и информационного окружения, б) Резервирование и восстановление информации

Должна быть обеспечена целостность программных средств СЗИ от НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алго-

ритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;

- целостность программной среды обеспечивается качеством приемки любых программных средств в АС.

Резервирование и восстановление информации.

Функции резервирования и восстановления информации, реализуемые в СЗИ от НСД, определяют, каким образом осуществляется резервное копирование данных (Рисунок 12).

Резервирование при условии защищенности от несанкционированного доступа резервных информационных носителей обеспечивает восстановление любых потерянных данных после реализации как случайных, так и преднамеренных угроз искажения или уничтожения информации.

Наиболее важными функциями резервирования информации являются:

1) Частота резервного копирования

Как правило, конфигурация предусматривает проведение полного резервного копирования данных один раз в неделю с дополнительным резервным копированием, проводимым в остальные дни. Дополнительное резервное копирование сохраняет только файлы, изменившиеся с момента последнего резервирования, что сокращает время процедуры и обеспечивает меньший объем пространства на резервном носителе.

2) Хранение резервных копий

Необходимо хранить носители с резервными копиями в защищенных местах, которые, тем не менее, должны быть доступны в случае, если потребуется восстановить утерянные данные. Например, в большинстве организаций предусмотрена ротация резервных носителей, согласно которой последние резервные ленты отключаются и помещаются в место хранения, а более ранние копии изымаются из хранилища для повторного использования. В данном случае ключевым параметром является скорость отключения и перемещения в место хранения. Это время зависит от степени опасности, представляемой для организации, если сбой произойдет в то время, когда резервный носитель будет отключен, от убытков вследствие хранения резервного носителя и времени, затрачиваемого на доставку носителей из места хранения. В организации должно быть установлено, насколько часто требуется применение резервных носителей для восстановления файлов. Если носители требуются каждый день, то, вероятно, имеет смысл хранить их несколько дней, пока не будет создана лента с более новой информацией.

3) Резервируемая информация

Не каждый файл на компьютере требует ежедневного резервного копирования. Например, исполняемые системные файлы и файлы конфигурации практически не меняются, поэтому для них не обязательно ежедневное резервирование. Имеет смысл создать резервную копию системных файлов заранее и загружать их с надежного носителя, если требуется переустановить систему.

Файлы данных, в особенности часто изменяющиеся, должны резервироваться регулярно. В большинстве случаев необходимо осуществлять их ежедневное резервное копирование.

Криптографическая подсистема

Функции криптографической системы представлены на рисунке 4.10.

Шифрование представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней (Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации. Это очень простой принцип. Вся сложность заключается в том, как реализуется весь этот процесс.

Рисунок 4.10 – а) Функции криптографической подсистемы,
б) Функции подсистемы антивирусной защиты.

Антивирусная защита рабочих станций и серверов.

Подсистема антивирусной защиты является неотъемлемой частью системы защиты СЗИ от НСД. При её правильной настройке значительно уменьшается риск воздействия вредоносных программ.

Но никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам.

В общем случае функциями подсистемы антивирусной защиты являются:

- Предотвращение заражения АРМ пользователя вредоносными программами;
- Обнаружение вредоносных программ;
- Удаление вредоносной программы из зараженного АРМ пользователя.

Глава 5. ПРОБЛЕМЫ ЭКСПЛУАТАЦИИ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

5.1. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.

Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:

- допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;
- на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;
- в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
- по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;
- изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;
- при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

Все носители информации на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном

или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.

Учет съемных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съемные накопители информации большой емкости или картриджи, съемные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота.

Съемные носители информации на магнитной или оптической основе в зависимости от характера или длительности использования допускается учитывать совместно с другими документами по установленным для этого учетным формам.

При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка "Для служебного пользования", номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.

5.4.6. Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.

5.4.7. Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

5.2. Защита конфиденциальной информации при эксплуатации автономных ПЭВМ

5.1.1 Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнитно-оптической) и бумажной основе.

В связи с этим порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.

5.5.2. АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" должны быть классифицированы и отнесены:

- к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
- ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.

Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости, классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном накопителе (либо одновременно используемом их комплексе).

5.3. Особенности защиты информации при использовании съемных накопителей информации большой емкости

5.1.2 Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.

В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнито-оптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.

Несъемные накопители должны быть исключены из конфигурации ПЭВМ.

Основной особенностью применения данной информационной технологии для АРМ на базе автономных ПЭВМ с точки зрения защиты информации является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите.

Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.

На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.

5.1.3 Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.

5.1.4 На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации.

В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть "закрыты на запись".

Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.

5.1.5 При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

5.1.6 Должна быть разработана и по согласованию с службой безопасности утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

5.4. Эксплуатация защищенных локальных вычислительных сетей

5.1.7 Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного сопровождения со стороны администратора безопасности информации.

5.1.8 Информация, составляющая служебную тайну, и персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в пунктах 5.8.4. и 5.8.5. следующего подраздела.

5.1.9 Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации".

5.1.10 Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации ЛВС.

5.1.11 Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

5.1.12 Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи.

5.5. Проблемы эксплуатации автоматизированных систем при межсетевом взаимодействии

5.1.13 Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Internet.

5.1.14 Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.

5.1.15 При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

5.1.16 Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

5.1.17 Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

- в АС класса 1Г - МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

5.6. Условия подключения абонентов к Сети

Подключение к Сети абонентского пункта (АП) осуществляется по решению руководителя учреждения (предприятия) на основании соответствующего обоснования.

5.1.18 Обоснование необходимости подключения АП к Сети должно содержать:

- наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;
- состав технических средств для оборудования АП;
- предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;
- режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);
- состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и т.п.);

- число и перечень предполагаемых абонентов (диапазон используемых IP- адресов);
- меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
- перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

5.1.19 Право подключения к Сети АП, не оборудованного средствами защиты информации от НСД, может быть предоставлено только в случае обработки на АП информации с открытым доступом, оформленной в установленном порядке как разрешенной к открытому опубликованию. В этом случае к АП, представляющим собой автономную ПЭВМ с модемом, специальные требования по защите информации от НСД не предъявляются.

5.1.20 Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД, отвечающих требованиям и рекомендациям, изложенным в подразделе 6.3.

5.1.21 Порядок подключения и взаимодействия абонентских пунктов с Сетью, требования и рекомендации по обеспечению безопасности информации.

Подключение АП к Сети должно осуществляться в установленном порядке через провайдера Сети.

5.1.22 Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде МЭ (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

5.1.23 Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления МЭ должны быть исключены из конфигурации.

5.1.24 АП с помощью МЭ должен обеспечивать создание сеансов связи абонентов с внешними серверами Сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

5.1.25 При использовании почтового сервера и Web-сервера предприятия, последние не должны входить в состав ЛВС АП и должны подключаться к Сети по отдельному сетевому фрагменту (через маршрутизатор).

5.1.26 На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для

выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном на предприятии порядке).

Не допускается активизация не включенных в обоснование прикладных серверов (протоколов) и не требующих привязок протоколов к портам.

5.1.27 Установку программного обеспечения, обеспечивающего функционирование АП, должны выполнять уполномоченные специалисты под контролем администратора. Абоненты АП не имеют права производить самостоятельную установку и модификацию указанного программного обеспечения, однако могут обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия "вирусов", замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения целиком ложится на абонента АП. При обнаружении фактов такого рода администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить рабочее место абонента от Сети и ЛВС и поставить об этом в известность руководство.

5.1.28 Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

5.1.29 СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;
- регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

5.1.30 Технические средства АП должны быть размещены либо в отдельном помещении (при автономной ПЭВМ, подключенной к Сети), либо в рабочих помещениях абонентов с принятием организационных и технических мер, исключающих несанкционированную работу в Сети. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки зрения электроакустики. В нерабочее время помещение автономной ПЭВМ либо соответствующего сервера сдается под охрану в установленном порядке.

5.1.31 При создании АП рекомендуется:

По возможности размещать МЭ для связи с внешними Сетями, Web-серверы, почтовые серверы в отдельном ЗП, доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы). Периодически проверять работоспособность МЭ с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не следует устанавливать на МЭ какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.).

При предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. Тем пользователям АП, которым не требуются услуги Сети, не предоставлять их. Пользователям, которым необходима только электронная почта (E-mail), предоставлять только доступ к ней. Максимальный перечень предоставляемых прикладных сервисов ограничивать следующими: E-mail, FTP, HTTP, Telnet.

При создании АП следует использовать операционные системы со встроенными функциями защиты информации от НСД, перечисленными в п.6.3.9, или использовать сертифицированные СЗИ НСД.

Эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов.

В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие "вирусов". Копии исходящей электронной почты и отсылаемых в Сеть файлов следует направлять в адрес защищенного архива АП для последующего анализа со стороны администратора (службы безопасности).

Проводить постоянный контроль информации, помещаемой на Web-серверы предприятия. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

Приказом по учреждению (предприятию) назначаются лица (абоненты), допущенные к работам в Сети с соответствующими полномочиями, лица, ответственные за эксплуатацию указанного АП и контроль за выполнением мероприятий по обеспечению безопасности информации при работе абонентов в Сети (руководители подразделений и администраторы).

5.1.32 Вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей:

- порядок подключения и регистрации абонентов в Сети;
- порядок установки и конфигурирования на АП общесистемного, прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, Browsers), их новых версий;
- порядок применения средств защиты информации от НСД на АП при взаимодействии абонентов с Сетью;
- порядок работы абонентов в Сети, в том числе с электронной почтой (E-mail), порядок выбора и доступа к внутренним и внешним серверам Сети (Web-серверам);
- порядок оформления разрешений на отправку данных в Сеть (при необходимости);
- обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с Сетью;
- порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов Сети.

К работе в качестве абонентов Сети допускается круг пользователей, ознакомленных с требованиями по взаимодействию с другими абонентами Сети и обеспечению при этом безопасности информации и допускаемых к самостоятельной работе в Сети после сдачи соответствующего зачета.

5.1.33 Абоненты Сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать инструкцию по обеспечению безопасности информации на АП;
- знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);
- уметь пользоваться средствами антивирусной защиты;
- после окончания работы в Сети проверить свое рабочее место на наличие "вирусов".

5.1.34 Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации учитываются в журналах несекретного делопроизводства. При этом на корпусе (конверте) носителя информации наносится предупреждающая маркировка: "Допускается использование только в Сети ____".

5.1.35 Для приемки в эксплуатацию АП, подключаемого к Сети, приказом по учреждению (предприятию) назначается аттестационная комиссия, проверяющая выполнение установленных требований и рекомендаций. Аттестационная комиссия в своей работе руководствуется требованиями и рекомендациями настоящего документа.

5.1.36 По результатам работы комиссии оформляется заключение, в котором отражаются следующие сведения:

- типы и номера выделенных технических средств АП, в т.ч. каждого абонента, их состав и конфигурация;
- состав общего и сервисного прикладного коммуникационного программного обеспечения (ОС, маршрутизаторов, серверов, межсетевых экранов, Browsers и т.п.) на АП в целом и на каждой рабочей станции абонента, в частности: логические адреса (IP-адреса), используемые для доступа в Сети;
- мероприятия по обеспечению безопасности информации, проведенные при установке технических средств и программного обеспечения, в т.ч. средств защиты информации от НСД, антивирусных средств, по защите информации от утечки по каналам ПЭМИН, наличие инструкции по обеспечению безопасности информации на АП.

5.1.37 При работе в Сети категорически запрещается:

- подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;
- изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;
- производить отправку данных без соответствующего разрешения;
- использовать носители информации с маркировкой: "Допускается использование только в Сети ____" на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

5.1.38 Ведение учета абонентов, подключенных к Сети, организуется в устанавливаемом в учреждении (на предприятии) порядке.

Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на администраторов АП, руководителей соответствующих подразделений, определенных приказом по учреждению (предприятию), а также руководителя службы безопасности.

5.7. Особенности защиты информации при эксплуатации системам управления базами данных

5.1.39 При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать информацию различного уровня конфиденциальности;
- разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
- разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
- регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;
- СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

5.1.40 С учетом указанных особенностей при создании БД рекомендуется:

- при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
- при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
- при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

Глава 6. ПОРЯДОК АТТЕСТАЦИИ И СЕРТИФИКАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

6.1. Аттестация автоматизированных систем

6.1.1. Общие положения

Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации (далее - федеральный орган по сертификации и аттестации), которым является Гостехкомиссия России.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного

доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью

специальной контрольной аппаратуры и тестовых средств;

- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Органы по аттестации аккредитуются Гостехкомиссией России. Правила аккредитации определяются действующим в системе "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Гостехкомиссия России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти.

Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители. Оплата работ по обязательной аттестации производится в соответ-

ствии с договором по утвержденным расценкам, а при их отсутствии - по договорной цене в порядке, установленном Гостехкомиссией России по согласованию с Министерством финансов Российской Федерации.

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители за счет финансовых средств, выделенных на разработку (доработку) и введение в действие защищаемого объекта информатизации.

Органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

6.1.2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации

Организационную структуру системы аттестации объектов информатизации образуют:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - Гостехкомиссия России;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

Федеральный орган по сертификации и аттестации осуществляет следующие функции:

- организует обязательную аттестацию объектов информатизации;
- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

- рассматривает апелляции, возникающие в процессе аттестации объектов информатизации и контроля за эксплуатацией аттестованных объектов информатизации;

- организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации.

Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

Органы по аттестации:

- аттестуют объекты информатизации и выдают "Аттестаты соответствия";

- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

- ведут информационную базу аттестованных этим органом объектов информатизации;

- осуществляют взаимодействие с Гостехкомиссией России и ежеквартально информируют его о своей деятельности в области аттестации.

Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с "Положением о сертификации средств защиты информации по требованиям безопасности информации".

Заявители:

проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

- привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

- предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

- привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на

аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

- осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";
- извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");
- предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

6.1.3. Порядок проведения аттестации и контроля

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработка программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрация и выдача "Аттестата соответствия";
- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации; - рассмотрение апелляций.

Подача и рассмотрение заявки на аттестацию

Заявитель для получения "Аттестата соответствия" заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации.

Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем и принимает решение о проведении аттестации объекта информатизации.

Предварительное ознакомление с аттестуемым объектом

При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предваритель-

ному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.

Испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте информатизации

При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

Испытания отдельных несертифицированных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации проводятся до аттестационных испытаний объектов информатизации.

В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения органов по сертификации средств защиты информации по требованиям безопасности информации и сертификаты.

Разработка программы и методики аттестационных испытаний

По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.

Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

Программа аттестационных испытаний согласовывается с заявителем.

6.1.4. Заключение договоров на аттестацию

Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по аттестации с привлекаемыми экспертами и

оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

Оплата работы членов аттестационной комиссии производится органом по аттестации в соответствии с заключенными трудовыми договорами (контрактами) за счет финансовых средств от заключаемых договоров на аттестацию объектов информатизации.

6.1.5. Проведение аттестационных испытаний объектов информатизации

На этапе аттестационных испытаний объекта информатизации:

- осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
- определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
- проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
- проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
- проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
- оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи "Аттестата соответствия" и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Оформление, регистрация и выдача "Аттестата соответствия".

"Аттестат соответствия" на объект информатизации, отвечающий требованиям по безопасности информации, выдается органом по аттестации.

"Аттестат соответствия" оформляется и выдается заявителю после утверждения заключения по результатам аттестации.

Регистрация "Аттестатов соответствия" осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору.

Ведение сводных информационных баз аттестованных объектов информатизации осуществляется Гостехкомиссией России или по ее поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов.

"Аттестат соответствия" выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче "Аттестата соответствия".

При этом может быть предложен срок повторной аттестации при условии устранения недостатков.

При наличии замечаний непринципиального характера "Аттестат соответствия" может быть выдан после проверки устранения этих замечаний.

6.1.6. Рассмотрение апелляций

В случае несогласия заявителя с отказом в выдаче "Аттестата соответствия" он имеет право обратиться в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

6.1.7. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации

Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации проводится Гостехкомиссией России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации - периодически в соответствии с планами работы по контролю и надзору.

Гостехкомиссия России может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органам по аттестации.

Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных и методических документов по безопасности информации, выявленных при контроле и надзоре, орган по аттестации может быть лишен лицензии на право проведения аттестации объектов информатизации.

При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и надзор, может быть приостановлено или аннулировано действие "Аттестата соответствия", с оформлением этого решения в "Аттестате соответствия" и информированием органа, ведущего сводную информационную базу аттестованных объектов информатики, и Гостехкомиссии России.

Решение об аннулировании действия "Аттестата соответствия" принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России, выявленных при контроле и надзоре и приведших к повторной аттестации, расходы по осуществлению контроля и надзора могут быть по решению Госарбитража взысканы с органа по аттестации. Повторная аттестация может быть также осуществлена за счет этого органа по аттестации.

Расходы по осуществлению надзора за обязательной аттестацией и эксплуатацией объектов, прошедших обязательную аттестацию, оплачиваются органом надзора из средств госбюджета, выделенных ему в этих целях.

6.1.8. Требования к нормативным и методическим документам по аттестации объектов информатизации

Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России.

Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

В нормативную документацию включаются только те показатели, характеристики, требования, которые могут быть объективно проверены.

В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые

средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

Тексты нормативных и методических документов, используемых при аттестации объектов информатизации, должны быть сформулированы ясно и четко, обеспечивая их точное и единообразное толкование. В них должно содержаться указание о возможности использования документа для аттестации определенных типов объектов информатизации по требованиям безопасности информации или направлений защиты информации.

6.2. Сертификация автоматизированных систем

6.2.1. Общие положения о системе сертификации автоматизированных систем

Сертификации в системе сертификации ФСТЭК России подлежат:

средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;

средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;

средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Сертификация средств защиты информации осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданием, заданием по безопасности, согласованными заявителями на сертификацию с ФСТЭК России (далее – требования по безопасности информации).

Система сертификации ФСТЭК России.

Участниками системы сертификации ФСТЭК России являются:

федеральный орган по сертификации;

организации, аккредитованные ФСТЭК России в качестве органа по сертификации (далее – органы по сертификации);

организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории (далее – испытательные лаборатории);

изготовители средств защиты информации.

ФСТЭК России в соответствии с подпунктами 13 и 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа

2004 г. N 1085, организует проведение сертификации средств защиты информации, разрабатывает и устанавливает в пределах своей компетенции требования по безопасности информации к средствам защиты информации, а также в соответствии с Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608, выполняет функции федерального органа по сертификации.

Органы по сертификации осуществляют сертификацию средств защиты информации, оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации (далее – сертификат соответствия).

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту сертификационных испытаний средств защиты информации и достоверность их результатов.

Изготовители разрабатывают и (или) производят средства защиты информации в соответствии с требованиями по безопасности информации.

Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну. [1]

Изготовители средств защиты информации ограниченного доступа, не составляющей государственную тайну, должны иметь лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. [2]

Заявителями на осуществление сертификации являются изготовители, а также федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления и организации, планирующие применять средства защиты информации.

Заявители должны обеспечивать соответствие сертифицированных средств защиты информации требованиям по безопасности информации, а также осуществлять устранение недостатков и дефектов средств защиты информации, в том числе устранение уязвимостей и недекларированных возможностей программного обеспечения средств защиты информации, информирование потребителей об обновлении программного обеспечения средств защиты информации, доведение до потребителей обновлений программного обеспечения средств защиты информации, а также изменений в эксплуатационную документацию (далее – техническая поддержка средств защиты информации).

6.2.2. Схемы сертификации

- Для единичного образца средства защиты информации – проведение испытаний образца средства защиты информации и проверки организации его технической поддержки.
- Для партии средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его технической поддержки.
- Для серийного производства средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его производства и технической поддержки.

Сертификация единичного образца или партии средства защиты информации организуется заявителем, планирующим применять средство защиты информации, в случае, если отсутствуют идентичные серийно производимые сертифицированные средства защиты информации.

Сертификация серийного производства средства защиты информации организуется заявителем, осуществляющим разработку и (или) производство средства защиты информации.

Сертификационные испытания средств защиты информации проводятся на материально-технической базе испытательной лаборатории, а также на материально-технических базах заявителя и (или) изготовителя, расположенных на территории Российской Федерации.

Срок действия сертификата соответствия не может превышать 5 лет. [1]

Сертификат соответствия выдается на срок, указанный в заявке на сертификацию.

По окончании срока действия сертификата соответствия заявитель вправе подать заявку на продление срока действия сертификата соответствия.

Средство защиты информации может применяться по окончании срока действия сертификата соответствия при условии соблюдения требований по безопасности информации и осуществления заявителем его технической поддержки.

Сертификация средств защиты информации осуществляется на основании договоров, заключаемых заявителем с испытательной лабораторией и органом по сертификации. [2]

Органы по сертификации, испытательные лаборатории должны обеспечивать защиту информации о средствах защиты информации, о требованиях по безопасности информации, методиках сертификационных испытаний в рамках систем менеджмента информационной безопасности.

Органы по сертификации и испытательные лаборатории на основании заключенных договоров обязаны обеспечивать защиту информации, обладателем которой является заявитель.

6.2.3. Порядок проведения сертификации автоматизированных систем

Сертификация средства защиты информации включает следующие процедуры:

- подача заявки на сертификацию;
- принятие решения о проведении сертификации средства защиты информации;
- сертификационные испытания средства защиты информации;
- оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия;
- выдача (отказ в выдаче) сертификата соответствия;
- предоставление дубликата сертификата соответствия;
- маркирование средств защиты информации;
- внесение изменений в сертифицированное средство защиты информации;
- переоформление сертификата соответствия;
- продление срока действия сертификата соответствия;
- приостановление действия сертификата соответствия;
- прекращение действия сертификата соответствия.

Подача заявки на сертификацию.

Заявитель при намерении сертифицировать средство защиты информации:

1) относит планируемое к сертификации средство защиты информации к одному из типов средств защиты информации, установленных требованиями по безопасности информации и подлежащих сертификации в системе сертификации ФСТЭК России;

2) определяет требования по безопасности информации, на соответствие которым планируется проведение сертификации средства защиты информации;

3) осуществляет производство (подготовку) образца (образцов) средства защиты информации;

4) готовит конструкторскую, программную и эксплуатационную документацию на средство защиты информации;

5) выбирает для проведения сертификационных испытаний средства защиты информации аккредитованную ФСТЭК России в соответствующей

области аккредитации испытательную лабораторию[1], согласовывает с ней возможность и сроки проведения сертификационных испытаний.

Для получения сертификата соответствия заявитель представляет в ФСТЭК России заявку на сертификацию.

В заявке на сертификацию указываются:

- наименование средства защиты информации;
- назначение средства защиты информации;
- полное и сокращенное (в случае, если имеется) наименование заявителя, его организационно-правовая форма;
- адрес местонахождения, почтовый адрес заявителя;
- номер и дата выдачи имеющейся у заявителя лицензии ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну, и (или) лицензии ФСТЭК России по разработке и производству средств защиты конфиденциальной информации (указывается заявителем, являющимся изготовителем);
- фамилия, имя и отчество (при наличии) руководителя заявителя;
- фамилия, имя и отчество (при наличии) лица, ответственного за сертификацию средства защиты информации;
- номер контактного телефона и адрес электронной почты (при наличии) заявителя;
- наименование лица (лиц), разработавшего (разработавших) средство защиты информации, адрес его (их) местонахождения (указываются при наличии такого лица (таких лиц));
- номер и дата выдачи имеющейся у разработчика (разработчиков) средства защиты информации лицензии ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну, и (или) лицензии ФСТЭК России по разработке и производству средств защиты конфиденциальной информации (для российских юридических лиц);
- наименование лица (лиц), обладающего (обладающих) исключительными правами на средство защиты информации, адрес его (их) местонахождения (указываются при наличии такого лица (таких лиц));
- наименование испытательной лаборатории, в которой планируется проведение сертификационных испытаний средства защиты информации;
- тип (типы) средств защиты информации, к которому (которым) относится представляемое на сертификацию средство защиты информации;
- документы, на соответствие требованиям которых должна проводиться сертификация средства защиты информации;
- схема сертификации средства защиты информации (при сертификации партии средства защиты информации указывается количество образцов средства защиты информации в партии);

- заявляемый срок действия сертификата соответствия;
- наименование лица, на материально-технической базе которого планируется проводить сертификационные испытания средства защиты информации, адрес места (адреса мест) проведения сертификационных испытаний.

Заявка на сертификацию должна быть подписана руководителем заявителя (лицом, которое в силу закона или учредительных документов выступает от его имени) и руководителем испытательной лаборатории.

Рекомендуемый образец заявки на сертификацию приведен в приложении N 1 к настоящему Положению.

К заявке на сертификацию прилагаются следующие документы:

- технические условия в двух экземплярах;
- техническое задание в двух экземплярах (в случае, если планируется проведение сертификации средства защиты информации на соответствие требованиям по безопасности информации, изложенным в техническом задании);
- задание по безопасности в двух экземплярах (в случае необходимости его разработки в соответствии с требованиями по безопасности информации);
- формуляр (паспорт) на средство защиты информации;
- договор с лицом (лицами), обладающим (обладающими) исключительными правами на средство защиты информации, о предоставлении заявителю права на сертификацию, эксплуатацию или производство средства защиты информации, а также на техническую поддержку средства защиты информации (прилагается в случае, если заявитель не обладает исключительными правами на средство защиты информации).

Заявка на сертификацию и прилагаемые к ней документы направляются заказным почтовым отправлением с уведомлением о вручении или представляются непосредственно в ФСТЭК России.

Заявка на сертификацию и прилагаемые к ней документы оформляются на русском языке. Допускается указывать на иностранном языке фирменное наименование средства защиты информации, наименования лица, разработавшего средство защиты информации, и лица, обладающего исключительными правами на средство защиты информации, а также адреса их местонахождения.

Принятие решения о проведении сертификации автоматизированных систем.

ФСТЭК России рассматривает заявку на сертификацию и прилагаемые к ней документы в течение месяца[1] со дня получения заявки на сертификацию.

Заявка на сертификацию и (или) прилагаемые к ней документы возвращаются для доработки в случае отсутствия сведений или документов, предусмотренных пунктами 20 и 21 настоящего Положения, а также в случае несоответствия документов, прилагаемых к заявке на сертификацию, требованиям по безопасности информации.

По итогам рассмотрения заявки на сертификацию и прилагаемых к ней документов в проведении сертификации средства защиты информации может быть отказано.

Основаниями для отказа в проведении сертификации средства защиты информации являются:

- несоответствие назначения средства защиты информации компетенции ФСТЭК России;
- отсутствие у заявителя и (или) изготовителя лицензии ФСТЭК России в случае, если наличие такой лицензии предусмотрено законодательством Российской Федерации;
- наличие в заявке на сертификацию и (или) в прилагаемых к ней документах недостоверных сведений;
- наличие в банке данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, сведений об уязвимостях средства защиты информации или поступивших в ФСТЭК России от уполномоченных органов сведений об угрозах безопасности, связанных с применением средства защиты информации.

Уведомление об отказе в проведении сертификации средства защиты информации или уведомление о необходимости доработки заявки на сертификацию и (или) прилагаемых к ней документов в срок не более трех дней со дня принятия решения подписывается уполномоченным должностным лицом ФСТЭК России и вручается заявителю или направляется ему заказным почтовым отправлением с уведомлением о вручении.

В случае принятия решения о проведении сертификации средства защиты информации в решении указываются:

- номер и дата принятия решения;
- наименование средства защиты информации;
- назначение средства защиты информации;
- полное и сокращенное (в случае, если имеется) наименование заявителя, его организационно-правовая форма, адрес местонахождения заявителя;
- наименование испытательной лаборатории, в которой будут проведены сертификационные испытания средства защиты информации;

- наименование органа по сертификации, в котором будет проведена сертификация средства защиты информации;
- документы, на соответствие требованиям которых должна проводиться сертификация средства защиты информации;
- схема сертификации средства защиты информации;
- наименование лица, на материально-технической базе которого планируется проводить сертификационные испытания средства защиты информации, адрес места (адреса мест) проведения сертификационных испытаний.

Решение о проведении сертификации средства защиты информации оформляется в четырёх экземплярах, подписывается уполномоченным должностным лицом ФСТЭК России и направляется заказным почтовым отправлением с уведомлением о вручении или вручается по одному экземпляру заявителю, испытательной лаборатории и органу по сертификации.

В случае сертификации средства защиты информации на соответствие требованиям по безопасности информации, изложенным в технических условиях, техническом задании или задании по безопасности, ФСТЭК России рассматривает и согласовывает технические условия, техническое задание или задание по безопасности, прилагаемые к заявке на сертификацию.

Один экземпляр технических условий, технического задания или задания по безопасности прикладывается к решению о проведении сертификации средства защиты информации и направляется заявителю.

В ходе проведения сертификации средства защиты информации в технические условия, техническое задание или задание по безопасности могут вноситься изменения по согласованию с ФСТЭК России.

Не допускается проводить сертификацию (сертификационные испытания) средства защиты информации до принятия решения о проведении сертификации средства защиты информации.

Заявитель должен в трехдневный срок письменно известить ФСТЭК России о заключении договоров с испытательной лабораторией и органом по сертификации с указанием определенного договорами срока проведения сертификации средства защиты информации.

Решение о проведении сертификации средства защиты информации подлежит переоформлению в случаях:

- изменения наименования средства защиты информации;
- замены испытательной лаборатории или органа по сертификации, в том числе в связи с приостановлением, прекращением действия аттестатов аккредитации испытательной лаборатории или органа по сертификации;
- изменения состава документов, на соответствие которым проводится сертификация средства защиты информации;

- изменения схемы сертификации средства защиты информации, в том числе изменения количества образцов в партии средств защиты информации;
- изменения места (мест) проведения сертификационных испытаний.

Обращение заявителя с обоснованием необходимости переоформления решения о проведении сертификации средства защиты информации направляется в ФСТЭК России заказным почтовым отправлением с уведомлением о вручении или представляется непосредственно в ФСТЭК России.

Решение о проведении сертификации средства защиты информации переоформляется в четырёх экземплярах в течение 10 рабочих дней со дня поступления обращения заявителя, подписывается уполномоченным должностным лицом ФСТЭК России и направляется заказными почтовыми отправлениями с уведомлением о вручении или вручается по одному экземпляру заявителю, испытательной лаборатории и органу по сертификации.

В случае отказа в переоформлении решения о проведении сертификации средства защиты информации уведомление с обоснованием отказа подписывается уполномоченным должностным лицом ФСТЭК России и вручается заявителю или направляется ему заказным почтовым отправлением с уведомлением о вручении.

Решение о проведении сертификации средства защиты информации аннулируется в случае:

- обращения заявителя о прекращении сертификации средства защиты информации;
- незаключения заявителем договоров с испытательной лабораторией и органом по сертификации на проведение сертификации по истечении 1 года с даты принятия решения о проведении сертификации средства защиты информации.

Уведомление об аннулировании решения о проведении сертификации средства защиты информации подписывается уполномоченным должностным лицом ФСТЭК России и направляется заказными почтовыми отправлениями с уведомлением о вручении или вручается заявителю, испытательной лаборатории и органу по сертификации.

Проведение сертификационных испытаний автоматизированных систем.

В целях подготовки к проведению сертификационных испытаний средства защиты информации заявитель представляет для предварительного рассмотрения в испытательную лабораторию и орган по сертификации следующую документацию на средство защиты информации:

- технические условия;
- задание по безопасности (в случае его разработки в соответствии с требованиями по безопасности информации);

- формуляр (паспорт) на средство защиты информации;
- иную конструкторскую (программную) и эксплуатационную документацию на средство защиты информации, предусмотренную требованиями по безопасности информации.

В целях соблюдения конфиденциальности информации о средстве защиты информации документация на средство защиты информации может быть представлена заявителем непосредственно на месте проведения сертификационных испытаний средства защиты информации.

Заявитель обязан предоставить возможность предварительного ознакомления испытательной лаборатории и органа по сертификации с образцом средства защиты информации.

В случае невозможности представления образца средства защиты информации в испытательную лабораторию и орган по сертификации по причине его массогабаритных характеристик или необходимости демонтажа, образец средства защиты информации может быть представлен заявителем непосредственно на месте проведения сертификационных испытаний средства защиты информации.

Испытательная лаборатория и орган по сертификации осуществляют предварительное рассмотрение образца средства защиты информации и документации на средство защиты информации в срок не более 45 календарных дней. Перечень выявленных недостатков с предложениями по их устранению направляется заявителю.

Если выявленные недостатки не могут быть устранены в сроки, предусмотренные договором на проведение сертификации средства защиты информации, орган по сертификации представляет в ФСТЭК России предложение об отказе в выдаче сертификата соответствия и извещает об этом заявителя.

Для проведения сертификационных испытаний средства защиты информации испытательная лаборатория разрабатывает программу и методику сертификационных испытаний средства защиты информации в соответствии с требованиями по безопасности информации и методическими документами, утвержденными ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

Программа и методика сертификационных испытаний средства защиты информации должны содержать описание средства защиты информации, количество образцов средства защиты информации, необходимых для проведения сертификационных испытаний, сроки проведения испытаний, правила отбора образцов средства защиты информации, состав и порядок

испытаний средства защиты информации, методы испытаний и применяемые средства, требования к конструкторской, программной и эксплуатационной документации.

Программа и методика сертификационных испытаний средства защиты информации согласовываются с заявителем и представляются на утверждение в орган по сертификации.

Орган по сертификации в течение 30 календарных дней рассматривает программу и методику сертификационных испытаний средства защиты информации и при отсутствии недостатков утверждает их.

В случае выявления недостатков орган по сертификации в течение трех календарных дней возвращает программу и методику сертификационных испытаний средства защиты информации в испытательную лабораторию на доработку, о чем уведомляет заявителя.

Испытательная лаборатория в течение 10 календарных дней устраняет недостатки, повторно согласовывает программу и методику сертификационных испытаний с заявителем и представляет их в орган по сертификации на утверждение.

Общий срок рассмотрения и утверждения программы и методики сертификационных испытаний средства защиты информации органом по сертификации не должен превышать 60 календарных дней.

Орган по сертификации письменно информирует ФСТЭК России об утверждении программы и методики сертификационных испытаний средства защиты информации.

Испытательная лаборатория осуществляет отбор образца (образцов) средств защиты информации, необходимых для проведения сертификационных испытаний.

При сертификации партии средства защиты информации для осуществления отбора образцов средства защиты информации должна быть представлена вся партия средства защиты информации.

При сертификации серийного производства средства защиты информации для осуществления отбора образцов средства защиты информации должна быть представлена партия средства защиты информации, численность которой не менее чем в два раза превышает количество образцов средства защиты информации, которое необходимо отобрать для проведения сертификационных испытаний.

Отбираемый образец (образцы) средства защиты информации по конструкции, составу и технологии изготовления должен (должны) соответствовать образцам средства защиты информации, предназначенным для реализации потребителю.

Объем выборки образцов средства защиты информации определяется исходя из условий статистической достоверности и с учетом затрат заяви-

теля в случае, если при проведении сертификационных испытаний возможен вывод из строя образца (образцов) средства защиты информации.

По результатам отбора составляется акт отбора образца (образцов) средства защиты информации, в котором указываются:

- номер и дата решения о проведении сертификации;
- дата осуществления отбора образца (образцов) средства защиты информации;
- наименование средства защиты информации;
- наименование заявителя;
- наименование испытательной лаборатории;
- фамилия, имя и отчество (при наличии) специалиста (специалистов) испытательной лаборатории, производившего (производивших) отбор образца (образцов) средства защиты информации;
- фамилия, имя и отчество (при наличии) специалиста (специалистов) заявителя, присутствовавшего (присутствовавших) при отборе образца (образцов) средства защиты информации;
- схема сертификации средства защиты информации (при сертификации партии средства защиты информации указывается количество образцов средства защиты информации в партии);
- количество образцов в партии средства защиты информации, представленной для осуществления отбора образца (образцов) средства защиты информации с указанием заводских номеров образцов средства защиты информации;
- количество отобранных образцов средства защиты информации, с указанием их заводских номеров;
- контрольные суммы программного обеспечения образца (образцов) средства защиты информации (при наличии программного обеспечения средства защиты информации).

Акт отбора образца (образцов) средства защиты информации подписывается специалистами заявителя и испытательной лаборатории, участвовавшими в отборе образца (образцов) средства защиты информации, и утверждается руководителем испытательной лаборатории.

Испытательная лаборатория проводит сертификационные испытания в соответствии с утвержденными органом по сертификации программой и методикой сертификационных испытаний средства защиты информации.

Орган по сертификации осуществляет контроль проведения сертификационных испытаний. Эксперт (эксперты) органа по сертификации может (могут) присутствовать при проведении сертификационных испытаний.

Сертификационные испытания включают:

- проведение испытаний отобранного образца (образцов) средства защиты информации, предусматривающих оценку соответствия параметров

и характеристик (функций безопасности информации) средства защиты информации требованиям по безопасности информации;

- проверку организации технической поддержки средства защиты информации, предусматривающую оценку соответствия работ (услуг) по технической поддержке средства защиты информации в ходе его эксплуатации, проводимых (предоставляемых) заявителем, требованиям по безопасности информации;
- проверку организации производства средства защиты информации, предусматривающую оценку соответствия работ по изготовлению средства защиты информации с целью подтверждения неизменности параметров и характеристик (функций безопасности информации) образцов серийно производимого средства защиты информации требованиям по безопасности информации (при сертификации производства средства защиты информации).

При проверке организации производства программных и программно-технических средств защиты информации проверяется внедрение заявителем процедур безопасной разработки программного обеспечения.

Сертификационные испытания проводятся в сроки, установленные договором, заключенным заявителем с испытательной лабораторией.

По результатам испытаний и проверок оформляются протоколы испытаний (проверок), содержащие основание для проведения испытаний (номер решения о проведении сертификации), даты и места проведения испытаний, описание испытываемого средства защиты информации, описание проведенных испытаний, результаты испытаний по каждому испытываемому параметру или характеристике (функции безопасности информации) средства защиты информации, выводы о соответствии (несоответствии) средства защиты информации, организации технической поддержки и производства средства защиты информации требованиям по безопасности информации.

Протоколы испытаний (проверок) подписываются специалистами испытательной лаборатории, проводившими сертификационные испытания.

По завершении испытаний и проверок, предусмотренных программой и методикой сертификационных испытаний средства защиты информации, оформляется техническое заключение о соответствии (несоответствии) средства защиты информации требованиям по безопасности информации, содержащее основание для проведения испытаний (номер решения о проведении сертификации), описание испытываемого средства защиты информации, требования, на соответствие которым проводились испытания, результаты испытаний, вывод о соответствии (несоответствии) средства защиты информации требованиям по безопасности информации.

Техническое заключение утверждается руководителем испытательной лаборатории.

В случае несоответствия средства защиты информации требованиям по безопасности информации техническое заключение направляется заявителю.

Заявитель должен устранить выявленные несоответствия средства защиты информации требованиям по безопасности информации и проинформировать об этом испытательную лабораторию в соответствии с договором на проведение сертификационных испытаний.

Сертификационные испытания проводятся в сроки, установленные договором, заключенным заявителем с испытательной лабораторией.

Повторные сертификационные испытания средства защиты информации проводятся в соответствии с договором на проведение сертификационных испытаний в объеме, необходимом для проверки устранения выявленных при проведении сертификационных испытаний несоответствий средства защиты информации требованиям по безопасности информации.

По результатам повторных сертификационных испытаний оформляются протоколы повторных испытаний (проверок) и техническое заключение.

Материалы сертификационных испытаний средства защиты информации представляются испытательной лабораторией в орган по сертификации.

Материалы сертификационных испытаний средства защиты информации должны включать:

- программу и методику сертификационных испытаний средства защиты информации, протоколы сертификационных испытаний средства защиты информации и техническое заключение;
- протоколы повторных сертификационных испытаний средства защиты информации и техническое заключение (в случае проведения повторных сертификационных испытаний);
- акт отбора образца (образцов) средства защиты информации;
- технические условия и извещение о внесении изменений в технические условия в двух экземплярах (в случае внесения таких изменений);
- дополнительное техническое задание в двух экземплярах (в случае проведения сертификации средства защиты информации на соответствие требованиям по безопасности информации, изложенным в техническом задании);
- задание по безопасности в двух экземплярах (в случае его разработки в соответствии с требованиями по безопасности информации);
- формуляр (паспорт) на средство защиты информации в двух экземплярах;
- дополнительную документацию на средство защиты информации, представленную заявителем при проведении сертификационных испытаний.

Все документы, за исключением дополнительной документации на средство защиты информации, представляются на бумажном носителе и в электронном виде. Дополнительная документация на средство защиты информации представляется только в электронном виде.

Оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия.

Орган по сертификации проводит оценку поступивших материалов сертификационных испытаний средства защиты информации на соответствие требованиям настоящего Положения и требованиям по безопасности информации, в том числе наличие в средстве защиты информации уязвимостей или недекларированных возможностей, несоответствие средства защиты информации требованиям по безопасности информации, наличие информации об угрозах безопасности, связанных с применением средства защиты информации.

Срок проведения оценки материалов сертификационных испытаний устанавливается договором между заявителем и органом по сертификации и не должен превышать 45 календарных дней с даты поступления в орган по сертификации всех документов, предусмотренных пунктом 52 настоящего Положения.

В случае непредставления документов, предусмотренных пунктом 52 настоящего Положения, орган по сертификации запрашивает их в испытательной лаборатории.

По результатам оценки материалов сертификационных испытаний средства защиты информации орган по сертификации оформляет экспертное заключение о возможности (невозможности) выдачи сертификата соответствия.

Экспертное заключение оформляется в трех экземплярах, подписывается всеми экспертами органа по сертификации, проводившими сертификацию (присутствовавшими при проведении сертификационных испытаний), и утверждается руководителем органа по сертификации.

Экспертное заключение должно содержать основание для проведения сертификации средства защиты информации (номер решения о проведении сертификации), наименование участников сертификации (заявителя, испытательной лаборатории и органа по сертификации), требования, на соответствие которым проведена сертификация средства защиты информации, результаты оценки материалов сертификационных испытаний, выводы о возможности (невозможности) выдачи сертификата соответствия.

В случае наличия в экспертном заключении вывода о возможности выдачи сертификата соответствия орган по сертификации подготавливает проект сертификата соответствия (рекомендуемый образец приведен в приложении N 3 к настоящему Положению).

Один экземпляр экспертного заключения, проект сертификата соответствия и материалы сертификационных испытаний, предусмотренные пунктом 52 настоящего Положения, представляются органом по сертификации в ФСТЭК России.

Экспертное заключение и проект сертификата соответствия представляются на бумажном носителе и в электронном виде.

Один экземпляр экспертного заключения направляется заявителю.

Выдача (отказ в выдаче) сертификата соответствия.

В случае если в экспертном заключении сделан вывод о невозможности выдачи сертификата соответствия, ФСТЭК России в срок не позднее 5 рабочих дней со дня поступления материалов по сертификации средства защиты информации принимает решение об отказе в выдаче сертификата соответствия.

В случае если в экспертном заключении сделан вывод о возможности выдачи сертификата соответствия, ФСТЭК России в срок не более 45 календарных дней рассматривает материалы по сертификации средства защиты информации и при отсутствии недостатков принимает решение о выдаче сертификата соответствия.

В случае выявления в материалах по сертификации средства защиты информации недостатков ФСТЭК России направляет материалы в орган по сертификации на доработку с приложением описания выявленных недостатков и предложениями по их устранению.

Уведомление о выявленных в материалах по сертификации средства защиты информации недостатках с их описанием и предложениями по устранению направляется испытательной лаборатории и заявителю.

Орган по сертификации, испытательная лаборатория и заявитель в срок не более 90 календарных дней со дня подписания уведомления должны устранить выявленные недостатки, при необходимости провести повторные сертификационные испытания средства защиты информации и представить в ФСТЭК России доработанные материалы по сертификации средства защиты информации.

В случае непредставления доработанных материалов по сертификации средства защиты информации ФСТЭК России принимает решение об отказе в выдаче сертификата соответствия.

Решение об отказе в выдаче сертификата соответствия подписывается уполномоченным должностным лицом ФСТЭК России и в течение 5 рабочих дней вручается заявителю или направляется ему заказным почтовым отправлением с уведомлением о вручении.

В случае принятия решения о выдаче сертификата соответствия сертификат соответствия подписывается уполномоченным должностным лицом ФСТЭК России, сведения о сертификате соответствия вносятся в государственный реестр сертифицированных средств защиты информации.

Сертификат соответствия в течение 10 рабочих дней после подписания вручается заявителю или направляется ему заказным почтовым отправлением с уведомлением о вручении.

Предоставление дубликата сертификата соответствия.

В случае утраты сертификата соответствия заявитель вправе обратиться в ФСТЭК России с заявлением о выдаче дубликата сертификата соответствия.

В течение 10 рабочих дней со дня регистрации заявления о выдаче дубликата сертификата соответствия ФСТЭК России оформляет дубликат на бланке сертификата соответствия с пометкой «дубликат, оригинал сертификата соответствия признается недействующим» и вручает заявителю или направляет ему заказным почтовым отправлением с уведомлением о вручении.

Маркирование средств защиты информации.

На основании сертификата соответствия заявитель организует маркирование средств защиты информации знаками соответствия.

В случае сертификации единичного образца средства защиты информации или партии средства защиты информации знаки соответствия направляются или выдаются заявителю вместе с сертификатом соответствия. Номера знаков соответствия указываются в сертификате соответствия.

В случае сертификации серийного производства средства защиты информации заявитель направляет в ФСТЭК России заявку на получение знаков соответствия, в которой указывает:

- наименование заявителя;
- наименование сертифицированного средства защиты информации;
- номер сертификата соответствия, дату его выдачи;
- количество знаков соответствия, необходимое для маркирования средства защиты информации.

ФСТЭК России рассматривает заявку на получение знаков соответствия в течение 5 рабочих дней.

Знаки соответствия вручаются заявителю или направляются ему заказным почтовым отправлением с уведомлением о вручении.

В случае наличия в заявке ошибочных или недостоверных сведений ФСТЭК России отказывает в предоставлении знаков соответствия, о чем уведомляет заявителя.

Маркирование средств защиты информации осуществляется только при наличии действующего сертификата соответствия.

Заявитель маркирует знаками соответствия каждый образец средства защиты информации, на которое выдан сертификат соответствия.

В случае прекращения производства и реализации средства защиты информации неиспользованные знаки соответствия подлежат возврату в ФСТЭК России. Маркирование иных, в том числе сертифицированных, средств защиты информации неиспользованными знаками соответствия не допускается.

Заявитель ведет журнал, в котором регистрирует промаркированные образцы средства защиты информации с указанием заводских номеров образцов средства защиты информации и номеров знаков соответствия.

Знаком соответствия маркируется корпус изделия (при наличии) или формуляр (паспорт) на средство защиты информации.

В формуляре (паспорте) на средство защиты информации указывается номер знака соответствия.

Маркирование средств защиты информации, являющихся программным обеспечением, распространяемым по сетям связи, осуществляется с применением электронной подписи или любым способом, подтверждающим подлинность средств защиты информации.

Внесение изменений в сертифицированное средство защиты информации.

Заявитель, являющийся разработчиком средства защиты информации, проводит испытания средства защиты информации с привлечением испытательной лаборатории в случае внесения в сертифицированное средство защиты информации изменений, связанных с добавлением новых функций безопасности информации, или изменений в имеющиеся функции безопасности информации.

В случае внесения в средство защиты информации иных изменений заявитель, являющийся разработчиком средства защиты информации, проводит испытания средства защиты информации самостоятельно или с привлечением испытательной лаборатории.

Заявитель, не являющийся разработчиком средства защиты информации, проводит испытания средства защиты информации с привлечением испытательной лаборатории в случае внесения в сертифицированное средство защиты информации изменений, связанных с добавлением новых функций безопасности информации, или изменений в имеющиеся функции безопасности информации и устранением уязвимостей (недекларированных возможностей) средства защиты информации.

В случае внесения в средство защиты информации иных изменений заявитель, не являющийся разработчиком средства защиты информации, проводит испытания средства защиты информации самостоятельно или с привлечением испытательной лаборатории.

В случае внесения в сертифицированное средство защиты информации изменений, связанных с устранением уязвимостей (недекларированных возможностей) средства защиты информации или обновлением баз дан-

ных, необходимых для реализации функций безопасности средства защиты информации, заявитель информирует потребителей о необходимости обновления средства защиты информации и доводит до потребителей обновления средства защиты информации до проведения испытаний, предусмотренных пунктами 71 и 72 настоящего Положения.

Испытания средства защиты информации в связи с внесением в него изменений, связанных с обновлением баз данных, необходимых для реализации функций безопасности средства защиты информации, проводятся в порядке, предусмотренном требованиями по безопасности информации.

По результатам проведенных испытаний средства защиты информации в связи с внесением в него изменений заявитель представляет в ФСТЭК России материалы испытаний, содержащие:

- техническое заключение;
- протоколы по результатам проведенных испытаний;
- технические условия и извещение о внесении изменений в технические условия в двух экземплярах (в случае внесения таких изменений);
- дополнительное техническое задание в двух экземплярах (в случае проведения сертификации средства защиты информации на соответствие требованиям по безопасности информации, изложенным в техническом задании, и в случае внесения изменений в техническое задание);
- задание по безопасности (при наличии) в двух экземплярах (в случае внесения изменений в задание по безопасности);
- формуляр (паспорт) на средство защиты информации и извещение о внесении изменений в формуляр (паспорт) в двух экземплярах (в случае внесения таких изменений).

ФСТЭК России течение 20 календарных дней рассматривает поступившие материалы испытаний, согласовывает технические условия, дополнительное техническое задание (при наличии) или задание по безопасности (при наличии) и формуляр (паспорт) на средство защиты информации, переоформляет сертификат соответствия.

Переоформление сертификата соответствия.

Сертификат соответствия подлежит переоформлению в случае:

а) реорганизации заявителя в форме преобразования;

б) изменения наименования заявителя;

в) изменения местонахождения заявителя;

г) внесения изменений в сертифицированное средство защиты информации, требующих внесения изменений в сертификат соответствия.

Для переоформления сертификата соответствия в случаях, указанных в подпунктах «а», «б» и «в» пункта 76 настоящего Положения, заявитель либо его правопреемник представляют в ФСТЭК России заявление о переоформлении сертификата соответствия.

В заявлении о переоформлении сертификата соответствия указываются новые сведения о заявителе или его правопреемнике.

Заявление о переоформлении сертификата соответствия представляется непосредственно в ФСТЭК России или направляется заказным почтовым отправлением с уведомлением о вручении.

ФСТЭК России в срок, не превышающий 10 рабочих дней со дня получения заявления о переоформлении сертификата соответствия, осуществляет проверку достоверности содержащихся в заявлении о переоформлении сертификата соответствия новых сведений и принимает решение о переоформлении сертификата соответствия или об отказе в его переоформлении.

Основаниями для отказа в переоформлении сертификата соответствия являются:

а) наличие в заявлении о переоформлении сертификата соответствия недостоверных сведений;

б) отсутствие у заявителя, занимающегося разработкой и (или) производством средства защиты информации, переоформленной лицензии ФСТЭК России в случае, если наличие такой лицензии предусмотрено законодательством Российской Федерации.

ФСТЭК России в случае отказа в переоформлении сертификата соответствия в течение 5 рабочих дней со дня принятия такого решения вручает заявителю или его правопреемнику уведомление об отказе в переоформлении сертификата соответствия с указанием причин отказа или направляет его заказным почтовым отправлением с уведомлением о вручении.

Уведомление о переоформлении сертификата соответствия с приложением переоформленного сертификата соответствия в течение 5 рабочих дней со дня принятия такого решения направляется заказным почтовым отправлением с уведомлением о вручении или вручается заявителю или его правопреемнику.

Заявитель в течение 5 рабочих дней со дня получения переоформленного сертификата соответствия должен представить (направить) в ФСТЭК России подлинник ранее выданного сертификата соответствия.

Продление срока действия сертификата соответствия.

В целях производства и реализации сертифицированного средства защиты информации срок действия сертификата соответствия может быть продлен в порядке, предусмотренном для сертификации средств защиты информации в соответствии с пунктами 19 – 61 настоящего Положения.

Приостановление действия сертификата соответствия.

Действие сертификата соответствия приостанавливается в случаях:

- изменения требований по безопасности информации;
- установления факта несоответствия сертифицированного средства защиты информации требованиям по безопасности информации на основа-

нии поступившей в ФСТЭК России информации, в том числе о наличии в сертифицированном средстве защиты информации уязвимостей или недекларированных возможностей;

- прекращения технической поддержки сертифицированного средства защиты информации, отсутствие которой может привести к несоответствию средства защиты информации требованиям по безопасности информации, а также к невыполнению требований о защите информации при применении средства защиты информации;
- обращения заявителя о приостановлении действия сертификата соответствия.

Решение о приостановлении действия сертификата соответствия оформляется приказом ФСТЭК России.

Действие сертификата соответствия может быть приостановлено на срок не более 90 календарных дней.

ФСТЭК России в течение 5 рабочих дней со дня принятия решения направляет заказным почтовым отправлением с уведомлением о вручении или вручает заявителю уведомление о приостановлении действия сертификата соответствия. В уведомлении указывается срок устранения несоответствия средства защиты информации требованиям по безопасности информации, который не должен превышать 90 календарных дней.

В случае приостановления действия сертификата соответствия заявитель должен прекратить производство и реализацию сертифицированного средства защиты информации.

Действие сертификата соответствия возобновляется в случае:

устранения несоответствия средства защиты информации требованиям по безопасности информации и представления в ФСТЭК России материалов, подтверждающих устранение несоответствия;

возобновления технической поддержки средства защиты информации;

обращения заявителя о возобновлении действия сертификата соответствия в случае, если решение о приостановлении действия сертификата соответствия было принято по обращению заявителя.

Решение о возобновлении действия сертификата соответствия оформляется приказом ФСТЭК России.

ФСТЭК России в течение 5 рабочих дней со дня принятия решения направляет заказным почтовым отправлением с уведомлением о вручении или вручает заявителю уведомление о возобновлении действия сертификата соответствия.

ФСТЭК России вносит сведения о приостановлении и возобновлении действия сертификата соответствия в государственный реестр сертифицированных средств защиты информации.

Прекращение действия сертификата соответствия.

Действие сертификата соответствия прекращается в случае:

- непредставления заявителем в установленный срок материалов, подтверждающих устранение несоответствия средства защиты информации требованиям по безопасности информации;
- невозобновления заявителем в установленный срок технической поддержки средства защиты информации;
- обращения заявителя о прекращении действия сертификата соответствия.

Решение о прекращении действия сертификата соответствия оформляется приказом ФСТЭК России.

ФСТЭК России в течение 5 рабочих дней со дня принятия решения направляет заказным почтовым отправлением с уведомлением о вручении или вручает заявителю уведомление о прекращении действия сертификата соответствия.

В случае прекращения действия сертификата соответствия заявитель должен прекратить производство и реализацию сертифицированного средства защиты информации, если такие мероприятия не были проведены в связи с приостановлением действия сертификата соответствия.

ФСТЭК России вносит сведения о прекращении действия сертификата соответствия в государственный реестр сертифицированных средств защиты информации.

ЗАКЛЮЧЕНИЕ

Представленный в учебном пособии материал по дисциплине «Информационная безопасность автоматизированных систем» является одним из специальных курсов в подготовке бакалавров по направлению «Информационная безопасность».

Цель учебного пособия – показать место и роль процесса создания, проектирования, разработки, внедрения, эксплуатации автоматизированных систем в защищенном исполнении в общей системе безопасности предприятия, достигнута.

По мнению авторов, важными являются вопросы особенности построения структуры, определение функций различных подразделений, эффективное использование современных методов управления как отдельных подразделений по защите информации, так и службы защиты информации в целом.

Успешное решение этих проблем возможно при наличии на предприятии специально подготовленных специалистов и организации работы по подбору, расстановке и использованию персонала как в службе защиты информации, так и во всех других подразделениях предприятия. Несомненно, наиболее особое внимание необходимо уделять подбору руководителей соответствующих служб.

ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

АРД – администратор разграничения доступа;
АРМ – автоматизированное рабочее место;
АУД – администратор управления доступом;
АС – автоматизированная система;
ВТ – вычислительная техника;
ИОД – информация ограниченного доступа;
КИ – конфиденциальная информация;
КСЗИ – комплексная система защиты информации.
МБО – монитор безопасности объектов;
МТО – материально-техническое обеспечение;
ОС – операционная система;
ПБ – политика безопасности;
ППР – подготовка и принятие решения;
ПРД – правила разграничения доступа;
СлЗи – служба защиты информации;
СВС – система военных сообщений;
СВТ – средство вычислительной техники;
ТЭО – технико-экономическое обоснование;
РРД – ролевое разграничение доступа;
ЭП – электронная подпись.

Аналитико-синтетическая обработка – преобразование документов в процессе их анализа и извлечения необходимой информации, а также оценка, сопоставление, обобщение и представление информации в виде, соответствующем запросу.

Библиографические исследования – это процесс получения нового знания на основе анализа документального потока, отражённого во вторичных изданиях.

Бизнес-справка – структурированная информация о фирме – потенциальном деловом партнёре, инвесторе, клиенте, конкуренте и предназначена для проверки надёжности фирмы.

Дайджесты – это фрагменты текстов многих документов (цитаты, выдержки, конспекты, реже рефераты), подобранные по определённой теме, не обеспеченной обобщающими публикациями, в логике и сфере интересов реальный или потенциальных потребителей.

Документальный поток – это совокупность функционирующих в обществе первичных документов.

Индивидуализация услуг – повседневная практика в сфере информационного обслуживания.

Информационная продукция – документы, информационные массивы, базы данных и информационные услуги, являющиеся результатом функционирования информационных систем, и направленная на удовлетворение информационных потребностей, что предполагает предоставление пользователю сведений, зафиксированных в документальном потоке.

Информационно-аналитическая деятельность – это создание нового знания на основе качественно содержательной обработки документальной информации с целью оптимизации принятия решения.

Информационные документы – документы, содержащие выводное знание в виде вводов, прогнозов, рекомендаций.

Информационные потребности – осознанная потребность в информации, необходимой для получения недостающих знаний.

Классифицирование – процесс обобщения и упорядочения, позволяет в компактной, сжатой и наглядной форме организовать и представить знания.

Коммуникативный аудит – это процесс выявления и анализа внешней и внутриорганизационной информации, прямо или косвенно характеризующей репутацию учреждения, его образ, сформировавшийся в представлении различных групп общественности и персонала.

Комплексные информационные мероприятия: выставки, презентации, ярмарки, Дни информации, Дни специалиста, бизнес-семинары, конференции, круглые столы, клубы по интересам и др. мероприятия. Назначение: научно-техническая пропаганда, культурно-просветительная деятельность, рекламная деятельность, мероприятия Public Relations, аналитико-коммуникативная деятельность.

Маркетинговые исследования – сбор и анализ информации о различных компонентах рынка в целях выработки организацией обоснованной рыночной стратегии.

Обзор – текстовое сообщение, содержащее сводную характеристику какого-либо вопроса или ряда вопросов, основанную на использовании информации, извлечённой из некоторого множества отобранных для этой цели документов за определённого время.

Патентные исследования – это исследования технического уровня и тенденций развития объектов хозяйственной деятельности, их патентоспособности, патентной чистоты, конкурентоспособности на основе патентной и другой информации.

Рынок информационных продуктов и услуг – совокупность экономических, правовых и организационных отношений, регулирующих их производство и потребление.

Сервис – любая разновидность общественно-полезного труда, направлена на удовлетворение разумных потребностей человека.

Социальная информация – это базовая, фундаментальная категория, определяющая и особенности потребностей людей, и возможности обслуживания, и цели деятельности библиотек или служб информации предприятий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алексенцев А.И. Каналы и методы несанкционированного доступа к конфиденциальной информации // Безопасность информационных технологий. – 2000. – № 3.

2. ГОСТ 19.301-79. ЕСПД. «Программа и методика испытаний. Требования к содержанию и оформлению».

3. ГОСТ РВ 51719-2001. «Испытания программной продукции. Общие положения».

4. ГОСТ 16504-81 «Испытание и контроль качества продукции».

5. ГОСТ РВ 15210-78 «Испытание опытных образцов и изделий. Основные положения».

6. ГОСТ 2.105-95. «Общие требования к текстовым документам».

7. Приказ ФСТЭК России № 55 от 3 апреля 2018г. «Об утверждении Положения по сертификации средств защиты информации».

8. «Положение о сертификации средств защиты информации по требованиям безопасности информации (приложение № 1 к приказу МО РФ № 058 1996 г.)»;

9. РД ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

10. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

11. ГОСТ 34.601-90 «Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»

12. Гришина Н.В., Мецатунян М.В., Русецкая И.А. Влияние социально-психологических аспектов на обеспечение информационной безопасности субъектов информационных отношений // Безопасность информационных технологий. – 2012. – №1. – С. 43–45.

13. Зайцев А.П. Технические средства и методы защиты информации. – М.: Горячая линия-Телеком, 2009. – 616 с.

14. Корнеев И.К., Степанов Е.А. Защита информации в офисе: учебник. – М.: Проспект, 2011. – 336 с.

15. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

16. Русецкая И.А. Роль подразделений конкурентной разведки в обеспечении информационной безопасности субъектов информационных

отношений // Тезисы докладов Всероссийской научно-практической конференции «Современные проблемы и задачи обеспечения информационной безопасности». – М.: Изд-во МФЮА, 2013. – С. 45–47.

17. «Об информации, информационных технологиях и защите информации»: Закон РФ от 27 июля 2006 г. № 149-ФЗ.

18. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации.– М.: НПЦ «Аналитика», 2008.– 436 с.

19. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие.– М.: Форум: Инфра-М, 2010.– 592 с.

20. Иванова С.В. Искусство подбора персонала: Как оценить человека за час. - 3-е изд. - М.: Альпина Бизнес Букс, 2006. - 160с.

21. Карташов С.А., Одегов Ю.Г., Кокорев И.А. Рекрутинг: наём персонала. - 2-е изд. – М.: Экзамен, 2003. – 320 с.

22. Кибанов А.Я. Управление персоналом организации: учебник. - 2-е изд., доп. и перераб. – М.: ИНФРА-М, 2002. – 638 с.

23. Робертс Г. Рекрутмент и отбор. Подход, основанный на компетенциях / пер. с англ. – М.: HIPPO, 2005. – 288 с.

24. Балашова Е. Рекрутмент. Неадекватный кандидат или работодатель? // Управление персоналом. – 2008. – № 22 (200). – С. 127.

25. Колосова М. Как оценить кандидата при подборе. Советы по формированию «золотого фонда» // Управление персоналом. – 2008. – № 4 (182). – С.132.

26. Горбунов А., Чуменко В. Выбор рациональной структуры средств защиты информации в АСУ. http://kiev-security.org.ua/box/2/26.shtml

27. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

28. ИСО/МЭК 15408-99 «Критерии оценки безопасности информационных технологий».

29. Козлов В. Критерии информационной безопасности и поддерживающие их стандарты: состояние и тенденции. «Стандарты в проектах современных информационных систем». Сборник трудов 2-й Всероссийской практической конференции. Москва, 27-28 марта 2002 года.

Учебное издание

Солодянников Александр Владимирович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Учебное пособие

Издано в авторской редакции

Подписано в печать 25.06.2020. Формат 60×84 1/16.
Усл. печ. л. 7,0. Тираж 50 экз. Заказ 2177.

Издательство СПбГЭУ. 191023, Санкт-Петербург, Садовая ул., д. 21.

Отпечатано на полиграфической базе СПбГЭУ