

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители  
Е. В. Прокопенко  
И. В. Чичерин

**ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА  
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Методические материалы**

Рекомендованы учебно-методической комиссией специальности 10.05.03  
Информационная безопасность автоматизированных систем в качестве  
электронного издания для использования в образовательном процессе

Кемерово 2018

## Рецензенты

Стенин Д. В. – кандидат технических наук, доцент директор ИИТМА

Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

**Прокопенко Евгения Викторовна**

**Чичерин Иван Владимирович**

**Программно-аппаратные средства обеспечения информационной безопасности:** методические материалы [Электронный ресурс] для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Электрон. издан. – Кемерово, 2018.

© КузГТУ, 2018

© Е. В. Прокопенко,  
И. В. Чичерин,  
составление, 2018

## Введение.

Средства обеспечения информационной безопасности предназначены:

- ✓ для защиты информации от вредоносного воздействия компьютерных вирусов, несанкционированного доступа, в том числе при межсетевом взаимодействии между информационными системами, для обнаружения компьютерных атак;
- ✓ для обеспечения конфиденциальности и целостности информации;
- ✓ для выявления уязвимостей и мониторинга инцидентов информационной безопасности;
- ✓ для резервного копирования и восстановления информации.

Выбор и применение средств обеспечения информационной безопасности осуществляются согласно требованиям законодательства Российской Федерации на основе классификации информационных систем с учетом моделей угроз и моделей нарушителя информационной безопасности.

Органам государственной власти субъектов Российской Федерации рекомендуется принимать дополнительные меры по повышению уровня защиты информационных ресурсов органов государственной власти и органов местного самоуправления, обратив особое внимание:

- ✓ на недопущение принятия и реализации региональных и муниципальных программ информатизации, в которых не предусмотрены меры по защите информации в соответствии с законодательством Российской Федерации;
- ✓ на обеспечение контроля за выполнением требований по защите информации при подключении к информационно-телекоммуникационным сетям международного информационного обмена информационно-телекоммуникационных сетей и информационных сетей, а также средств вычислительной техники, применяемых для обработки информации ограниченного доступа;
- ✓ на кадровое усиление подразделений по защите информации.

### **Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки. Правовые, нормативно-технические и организационные требования к средствам защиты информации.**

Конечной целью создания системы обеспечения безопасности информационных технологий является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) АС соответствующими множеством значимых угроз методами и средствами.

Обеспечение информационной безопасности – это непрерывный процесс, основное содержание которого составляет управление, – управление людьми, рисками, ресурсами, средствами защиты и т.п. Люди – обслуживающий персонал и конечные пользователи АС, – являются неотъемлемой частью автоматизиро-

ванной (то есть «человеко-машинной») системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

- **сотрудников структурных подразделений** (конечных пользователей АС), решающих свои функциональные задачи с применением средств автоматизации;

- **программистов**, осуществляющих разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации;

- **сотрудников подразделения внедрения и сопровождения ПО**, обеспечивающих нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ (задач);

- **сотрудников подразделения эксплуатации ТС**, обеспечивающих нормальную работу и обслуживание технических средств обработки и передачи информации и системного программного обеспечения;

- **системных администраторов** штатных средств защиты (ОС, СУБД и т. п.);

- **сотрудников подразделения защиты информации**, оценивающих состояние информационной безопасности, определяющих требования к системе защиты, разрабатывающих организационно-распорядительные документы по вопросам ОИБ (аналитиков), внедряющих и администрирующих специализированные дополнительные средства защиты (администраторов безопасности);

- **руководителей организации**, определяющих цели и задачи функционирования АС, направления ее развития, принимающих стратегические решения по вопросам безопасности и утверждающих основные документы, регламентирующие порядок безопасной обработки и использования защищаемой информации сотрудниками организации.

Кроме того, на информационную безопасность организации могут оказывать влияние **посторонние лица** и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АС или несанкционированного доступа к информации как локально, так и удаленно.

#### **Регламентация действий пользователей и обслуживающего персонала АС**

Обслуживающий персонал и пользователи, как неотъемлемая часть АС, сами являются источником внутренних угроз информационной безопасности организации и одновременно могут являться частью системы защиты АС. Поэтому одним из основных направлений ОИБ является регламентация действий всех пользователей и обслуживающего персонала АС, целями которой являются:

- сокращение возможностей лиц из числа пользователей и персонала по совершению нарушений (как неумышленных, так и преднамеренных);

- реализацию специальных мер противодействия другим внутренним и внешним для системы угрозам (связанным с отказами и сбоями оборудования, ошибками в программах, стихийными бедствиями и действиями посторонних лиц, не являющихся частью АС).

Кроме того, чтобы персонал и пользователи как часть системы безопасности АС реализовали свои «защитные возможности», регламентации подлежат вопросы исполнения ими дополнительных специальных обязанностей (функций), свя-

занных с усилением режима информационной безопасности. Так, для защиты от действий посторонних лиц и «подкрепления» вводимых ограничений на действия своих сотрудников на компьютерах АС могут применяться средства защиты, работающие на физическом, аппаратном или программном уровне. Применение таких средств защиты требует регламентации вопросов их использования конечными пользователями и процессов их администрирования сотрудниками подразделений автоматизации и обеспечения информационной безопасности.

С учетом всего сказанного выше, можно сделать вывод: к обеспечению безопасности информационных технологий организации (и в определенной степени к управлению ее информационной безопасностью) должны привлекаться практически все сотрудники, участвующие в процессах автоматизированной обработки информации, и все категории обслуживающего АС персонала.

За формирование системы защиты и реализацию единой политики информационной безопасности организации и осуществление контроля и координации действий всех подразделений и сотрудников организации по вопросам ОИБ должно непосредственно отвечать специальное подразделение (служба) защиты информации (обеспечения информационной безопасности).

В силу малочисленности данного подразделения решение им многих процедурных вопросов и эффективный контроль за соблюдением всеми сотрудниками требований по ОИБ возможны только при назначении во всех подразделениях, эксплуатирующих подсистемы АС, штатных помощников – ответственных за обеспечение информационной безопасности.

Эффективное использование штатных (для ОС и СУБД) и дополнительных средств защиты обеспечивается системными администраторами и администраторами средств защиты. Системные администраторы обычно входят в штат подразделений автоматизации (информатизации). Администраторы дополнительных средств защиты, как правило, являются сотрудниками подразделения защиты информации.

Таким образом, организационную структуру системы обеспечения информационной безопасности АС организации можно представить в виде, совокупности следующих уровней:

- уровень 1 – Руководство организации
- уровень 2 – Подразделение ОИБ
- уровень 3 – Администраторы штатных и дополнительных средств защиты
- уровень 4 – Ответственные за ОИБ в подразделениях (на технологических участках)
- уровень 5 – Конечные пользователи и обслуживающий персонал

### **Понятие технологии обеспечения информационной безопасности**

Под *технологией обеспечения информационной безопасности в АС* понимается определенное распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников

(должностных лиц) организации по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.

Требования к технологии управления безопасностью:

- соответствие современному уровню развития информационных технологий;
- учет особенностей построения и функционирования различных подсистем

АС;

- точная и своевременная реализация политики безопасности организации;
- минимизация затрат на реализацию самой технологии обеспечения безопасности.

Для реализации технологии обеспечения безопасности в АС необходимо:

- наличие полной и непротиворечивой правовой базы (системы взаимосвязанных нормативно – методических и организационно-распорядительных документов) по вопросам ОИБ;

- распределение функций и определение порядка взаимодействия подразделений и должностных лиц организации по вопросам ОИБ на всех этапах жизненного цикла подсистем АС, обеспечивающее четкое разделение их полномочий и ответственности;

- наличие специального органа (подразделения защиты информации, обеспечения информационной безопасности), наделенного необходимыми полномочиями и непосредственно отвечающего за формирование и реализацию единой политики информационной безопасности организации и осуществляющего контроль и координацию действий всех подразделений и сотрудников организации по вопросам ОИБ.

Реализация технологии ОИБ предполагает:

- назначение и подготовку должностных лиц (сотрудников), ответственных за организацию, реализацию функций и осуществление конкретных практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

- строгий учет всех подлежащих защите ресурсов системы (информации, ее носителей, процессов обработки) и определение требований к организационно-техническим мерам и средствам их защиты;

- разработку реально выполнимых и непротиворечивых организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- реализацию (реорганизацию) технологических процессов обработки информации в АС с учетом требований по информационной безопасности;

- принятие эффективных мер сохранности и обеспечения физической целостности технических средств и поддержку необходимого уровня защищенности компонентов АС;

- применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывную административную поддержку их использования;

- регламентацию всех процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников структурных подразделений, использующих АС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, на ос-

нове утвержденных организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- четкое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- персональную ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;

- эффективный контроль за соблюдением сотрудниками подразделений – пользователями и обслуживающим АС персоналом – требований по обеспечению безопасности информации;

- проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработку и реализацию предложений по совершенствованию системы защиты информации в АС.

Организационные (административные) меры регламентируют процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

### **Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты**

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. Они включают:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;

- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);

- периодически проводимые (через определенное время) мероприятия;

- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

### **Разовые мероприятия**

К разовым мероприятиям относят:

- мероприятия по созданию нормативно-методологической базы (разработка концепции и других руководящих документов) защиты АС;

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т. п.);

- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т. п.);

- проведение спецпроверок применяемых в АС средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;

- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, технологические инструкции пользователей системы и т. п.) по вопросам обеспечения безопасности ресурсов АС и действиям в случае возникновения кризисных ситуаций;

- создание подразделения защиты информации (компьютерной безопасности) и назначение штатных ответственных за ОИБ в подразделениях и на технологических участках, осуществляющих организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации; разработка и утверждение их функциональных обязанностей;

- мероприятия по разработке политики безопасности, определение порядка назначения, изменения, утверждения и предоставления конкретным категориям сотрудников (должностным лицам) необходимых полномочий по доступу к ресурсам системы;

- мероприятия по созданию системы защиты АС и необходимой инфраструктуры (организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией, оборудование служебных помещений сейфами (шкафами) для хранения реквизитов доступа, средствами уничтожения бумажных и магнитных носителей конфиденциальной информации и т.п.);

- мероприятия по разработке правил разграничения доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием АС, а также используемых при их решении режимов обработки и доступа к данным;

- определение перечней файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требований к уровням их защищенности от НСД при передаче, хранении и обработке в АС;

- выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процессов обработки информации и каналов доступа к ней, оценка возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);

- организация охраны и надежного пропускного режима;

- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих

местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто

- контролирует и что при этом они должны делать), определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;

- определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

### **Периодически проводимые мероприятия**

К периодически проводимым мероприятиям относят:

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т. п.);

- анализ системных журналов (журналов регистрации), принятие мер по обнаруженным нарушениям правил работы;

- пересмотр правил разграничения доступа пользователей к ресурсам АС организации;

- осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты и разработка необходимых мер по совершенствованию (пересмотру состава и построения) системы защиты.

### **Мероприятия, проводимые по необходимости**

К мероприятиям, проводимым по необходимости, относят:

- мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;

- мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (санкционирование, рассмотрение и утверждение изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т. п.);

- проверка поступающего оборудования, предназначенного для обработки закрытой информации, на наличие специально внедренных закладных устройств, инструментальный контроль технических средств на наличие побочных электромагнитные излучения и наводок;

- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи;

- мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.);

- оформление юридических документов (договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами) и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с информационным обменом;
- обновление технических и программных средств защиты от НСД к информации в соответствии с меняющейся оперативной обстановкой.

### **Постоянно проводимые мероприятия**

Постоянно проводимые мероприятия включают:

- мероприятия по обеспечению) достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т. п.).
- мероприятия по непрерывной поддержке функционирования и управлению (администрированию) используемыми средствами защиты;
- организацию явного и скрытого контроля за работой пользователей и персонала системы;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй, функционирования, обслуживания и ремонта АС;
- постоянно (силами службы безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

### **Распределение функций по ОИБ**

Реализация подразделениями и отдельными сотрудниками организации функций по ОИБ осуществляется в соответствии с разработанными и утвержденными руководством организационно-распорядительными документами (положениями, инструкциями, обязанностями, перечнями, формулярами и т.п.), о которых говорилось выше.

Приведенное далее структурное деление и наименование подразделений являются условными и введены с целью конкретизации положений Технологии.

Технология управления информационной безопасностью предусматривает взаимодействие и реализацию определенных функций по ОИБ следующими подразделениями и должностными лицами организации:

#### **Служба безопасности (отдел защиты информации)**

Выполнение различных мероприятий по созданию и поддержанию работоспособности системы защиты должно быть возложено на специальную службу – службу компьютерной безопасности.

Служба обеспечения безопасности информации должна представлять собой систему штатных подразделений и нештатных сотрудников, организующих и обеспечивающих комплексную защиту информации.

На основе утвержденной системы организационно-распорядительных документов подразделения выполняют следующие основные действия:

- определяет критерии, по которым различные АРМ относятся к той или иной категории по требуемой степени защищенности, и оформляет их в виде «Положения об определении требований по защите (категорировании) ресурсов»;
- определяет типовые конфигурации и настройки программно-аппаратных средств защиты информации для АРМ различных категорий (требуемых степеней защищенности);
- по заявкам руководителей подразделений (используя формуляры АРМ и формуляры задач) проводит анализ возможности решения (а также совмещения) указанных задач на конкретных АРМ (с точки зрения обеспечения безопасности) и принимает решение об отнесении АРМ к той или иной группе по степени защищенности;
- совместно с отделом технического обслуживания Управления автоматизации проводит работы по установке на АРМ программно-аппаратных средств защиты информации;
- согласовывает и утверждает предписания на эксплуатацию АРМ (формуляры АРМ), подготовленные в подразделениях организации;
- обеспечивает проведение необходимых дополнительных специальных мероприятий по обеспечению безопасности информации;
- определяет организацию, методики и средства контроля эффективности противодействия попыткам несанкционированного доступа к информации (НСД) и незаконного вмешательства в процесс функционирования АС.

#### **Управление автоматизации (отдел эксплуатации и отдел телекоммуникаций)**

- по заявкам руководителей подразделений (используя формуляры АРМ и формуляры задач) проводит анализ возможности решения указанных задач на конкретных АРМ и уточнение содержания необходимых для этого изменений в конфигурации аппаратных и программных средств АРМ;
- на основе утвержденных заявок начальников подразделений установленным порядком производит:
  - установку (развертывание, обновление версий) программных средств, необходимых для решения на АРМ конкретных задач (используя полученные в ФАП дистрибутивы и формуляры задач);
  - удаление (затирание) программных пакетов, необходимость в использовании которых отпала;
  - установку (развертывание) новых АРМ (ПЭВМ) или подключение дополнительных устройств (узлов, блоков), необходимых для решения на АРМ конкретных задач;

- изъятие или замену ПЭВМ (отдельных устройств, узлов, блоков), необходимость в использовании которых отпала, предварительно осуществляя установленным порядком затирание остаточной информации на изымаемых машинных носителях;

- принимает участие в заполнении (корректировке сведений) формуляров АРМ и выдаче предписаний к эксплуатации АРМ;

- в своей деятельности сотрудники отдела эксплуатации руководствуются «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АРМ АС организации».

### **Управление автоматизации (фонд алгоритмов и программ – ФАП)**

- ведет общий перечень задач, решаемых в АС организации;

- по запросу начальников подразделений организации предоставляет общий перечень и копии формуляров конкретных задач, решаемых в АС;

- совместно с отделами разработки и сопровождения Управления автоматизации и отделом защиты информации оформляет формуляры установленного образца на новые функциональные задачи АС, сдаваемые в ФАП;

- хранит установленным порядком и осуществляет резервное копирование и контроль целостности лицензионных дистрибутивов или эталонных носителей, принятых в ФАП программных пакетов;

- осуществляет выдачу установленным порядком (во временное пользование) специалистам отдела технического обслуживания Управления автоматизации лицензионных дистрибутивов или эталонных носителей программных пакетов (их целостных копий) для их развертывания или обновления на АРМ АС организации по заявкам начальников отделов.

### **Все управления и отделы (структурные подразделения) организации**

- определяют функциональные задачи, которые должны решаться в подразделении с использованием АРМ АС организации;

- все необходимые изменения в конфигурации АРМ и полномочиях пользователей подразделения осуществляют на основе заявок в соответствии с «Инструкцией по внесению изменений в списки пользователей АС организации и наделению их полномочиями доступа к ресурсам системы» и «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АРМ автоматизированной системы организации»;

- заполняют формуляры АРМ и представляют их на утверждение в отдел технической защиты Управления безопасности;

- обеспечивают надлежащую эксплуатацию установленных на АРМ средств защиты информации.

## **Система организационно-распорядительных документов по организации комплексной системы защиты информации**

В Уставе организации (основном документе, в соответствии с которым организация осуществляет свою деятельность), во всех положениях о структурных подразделениях организации (департаментов, управлений, отделов, служб, групп, секторов и т. п.) и в функциональных обязанностях всех сотрудников, участвующих в процессах автоматизированной обработки информации, должны быть отражены требования по обеспечению информационной безопасности при работе в АС.

Задачи организации и функции по ОИБ ее подразделений и сотрудников в перечисленных выше документах должны формулироваться с учетом положений действующего в России законодательства по информатизации и защите информации (Федеральных Законов, Указов Президента РФ, Постановлений Правительства РФ и других нормативных документов).

Конкретизация задач и функций структурных подразделений, а также детальная регламентация действий сотрудников организации, их ответственность и полномочия по вопросам ОИБ при эксплуатации АС должны осуществляться как путем дополнения существующих документов соответствующими пунктами, так и путем разработки и введения в действие дополнительных внутренних организационно-распорядительных документов по ОИБ.

В целях обеспечения единого понимания всеми подразделениями и должностными лицами (сотрудниками) организации проблем и задач по обеспечению безопасности информации в организации целесообразно разработать *«Концепцию обеспечения информационной безопасности»* организации. В Концепции на основе анализа современного состояния информационной инфраструктуры организации и интересов организации в области обеспечения безопасности должны определяться основные задачи по защите информации и процессов ее обработки, намечаться подходы и основные пути решения данных задач.

Необходимым элементом организации работ по обеспечению безопасности информации, ее носителей и процессов обработки в АС организации является категорирование, то есть определение требуемых степеней защищенности (категорий) ресурсов АС (информации, задач, каналов взаимодействия задач, компьютеров). Для обеспечения управления и контроля за соблюдением установленных требований к защите информации и с целью обеспечения дифференцированного подхода к защите конкретных АРМ различных подсистем АС организации необходимо разработать и принять *«Положение об определении требований по защите (категорировании) ресурсов»* в АС организации. В этом документе необходимо отразить вопросы взаимодействия подразделений организации при определении требуемой степени защищенности ресурсов АС организации в зависимости от степени ценности обрабатываемой информации, характера обработки и обязательств по ОИБ перед сторонними организациями и физическими лицами.

Целесообразно введение классификации защищаемой информации, включаемой в *«Перечень информационных ресурсов, подлежащих защите»*, не только по уровню конфиденциальности (конфиденциально, строго конфиденциально

и т.д.), но и по уровню ценности информации (определяемой величиной возможных прямых и косвенных экономических потерь в случае нарушения ее целостности и несвоевременности представления – своевременности решения задач).

В данном Перечне необходимо также указывать подразделения организации, являющиеся владельцами конкретной защищаемой информации и отвечающие за установление требований к режиму ее защиты.

Любые изменения состава и полномочий пользователей подсистем АС должны производиться установленным порядком согласно специальной *«Инструкции по внесению изменений в списки пользователей АС и наделению их полномочиями доступа к ресурсам системы»*.

Меры безопасности при вводе в эксплуатацию новых рабочих станций и серверов, а также при изменениях конфигурации технических и программных средств существующих компьютеров в АС должны определяться *«Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств компьютеров АС»*.

Разработка ПО задач (комплексов задач), проведение испытаний разработанного и приобретенного ПО, передача ПО в эксплуатацию должна осуществляться в соответствии с утвержденным *«Порядком разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию»*.

*«Инструкция по организации антивирусной защиты»* должна регламентировать организацию защиты АС от разрушающего воздействия компьютерных вирусов и устанавливать ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС, за их ненадлежащее выполнение.

*«Инструкция по организации парольной защиты»* призвана регламентировать процессы генерации, смены и прекращения действия паролей пользователей в автоматизированной системе организации, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

При использовании в некоторых подсистемах АС средств криптографической защиты информации и средств электронной цифровой подписи необходим еще один документ, регламентирующий действия конечных пользователей, – *«Порядок работы с носителями ключевой информации»*.

Для пользователей защищенных АРМ (на которых обрабатывается защищаемая информация или решаются подлежащие защите задачи и на которых установлены соответствующие средства защиты) должны быть разработаны необходимые *дополнения к функциональным обязанностям и технологическим инструкциям*, закрепляющие требования по обеспечению информационной безопасности при работе в АС и ответственность сотрудников за реализацию мер по обеспечению установленного режима защиты информации.

Регламентация предусматривает введение таких ограничений и внедрение таких приемов работы сотрудников, которые, не создавая помех для исполнения ими своих функциональных обязанностей (технологических функций), минимизируют возможности.

## **Подсистема контроля доступа пользователей к ресурсам.**

Изобретение относится к информационным вычислительным системам и сетям. Технический результат заключается в повышении уровня защиты рабочих станций и серверов. Устройство содержит блок авторизации пользователя, блок разграничения прав доступа, блок хранения прав доступа, блок авторизации администратора безопасности, блок таймера, блок добавочного разграничения прав доступа, блок хранения эталонных настроек прав доступа, блок сравнения прав доступа с эталоном, блок формирования и восстановления текущих прав доступа. 3 ил.

Изобретение относится к вычислительной технике, а именно к информационным вычислительным системам и сетям, и может быть использовано в части контроля доступа к информационным ресурсам рабочих станций и серверов в сложных информационных системах, отличающихся иерархией задач администрирования информационной безопасности.

Известна система контроля доступа к информационным ресурсам, в частности к таблицам данных, входящая в состав СУБД, например, Oracle, MS SQL (см. Галатенко В.А. Информационная безопасность – основы//СУБД, 1996, 1). Она представляет собой программный комплекс, входящий в состав ПО СУБД.

Наиболее близкой по технической сущности к заявляемой (прототипом) является система контроля доступа к информационным ресурсам, в частности к разделяемым ресурсам, используемая в составе ОС, в частности в ОС Windows 9x/NT (см. кн. Валда Хиллей "Секреты Windows NT Server 4.0". – Киев: Диалектика, 1997, с. 14–15). Она представляет собой программный комплекс, выполненный для ОС Windows 9x/NT в виде отдельного драйвера, в ОС Unix входит в состав ядра.

Система контроля доступа к информационным ресурсам представлена на фиг. 1. Система содержит блок авторизации пользователя 1, блок разграничения прав доступа 2, блок хранения прав доступа 3, причем первый вход/выход блока авторизации пользователя 1 соединен со входом/выходом авторизации пользователя 4, второй вход/выход – с первым входом/выходом блока хранения прав доступа 3, второй вход/выход которого – со входом/выходом блока разграничения прав доступа 2, первый вход которого – с выходом блока авторизации пользователя 1, второй вход – со входом запроса доступа 5, первый выход – с выходом разрешения доступа 7, второй выход – с первым входом блока хранения прав доступа 3, второй вход которого – со входом задания параметров доступа 6.

Работает система следующим образом. Перед началом работы пользователь должен пройти авторизацию со входа 4, которая осуществляется блоком 1, параметры авторизации – имя и пароль пользователя блок 1 запрашивает и получает от блока 3. Данные текущего пользователя блоком 1 выдаются в блок 2, которым запрашиваются в блоке 3 таблица разграничения прав доступа зарегистрированного в системе пользователя. При запросе пользователем доступа к информационным ресурсам со входа 5 (запрашивается объект доступа, например, файл и действия, например, чтение или запись) блок 2 анализирует заданные для пользователя права доступа и запрашиваемые пользователем параметры доступа, если

они не противоречивы – запрашиваемый доступ системой разрешен, вырабатывается сигнал разрешения доступа к информационному ресурсу, выдаваемый на выход 7. Со входа 6 задаются параметры прав доступа, изменять данные права разрешается пользователю, имеющему соответствующие полномочия – если выдается соответствующий сигнал со второго выхода блока 2, формируемый после авторизации пользователя и его запроса (со входа 5) на получение доступа к блоку 3 (блок 3 в общем случае также является файловым объектом).

К недостаткам системы можно отнести следующее.

В общем случае в сложной информационной системе может присутствовать несколько уровней иерархии, к которым можно отнести системный уровень, уровень СУБД и уровень приложений. На каждом уровне решаются задачи контроля доступа к информационным ресурсам, собственными средствами – для каждого уровня реализована собственная система, представленная на фиг.1, администрирование которыми осуществляется администраторами соответствующих уровней – системным администратором, администратором СУБД, администратором приложений (некоторые задачи, например, создание разделяемого ресурса для ОС Windows 95/98 вообще решаются пользователем). Для обеспечения информационной безопасности сложной системы должна обеспечиваться централизация администрирования средствами защиты информации. Однако в данном случае, это невозможно, ввиду того, что централизация может быть достигнута только в случае, если администратор безопасности будет сам осуществлять администрирование безопасностью системы на всех ее уровнях иерархии (это неприемлемо сложная задача и не всегда достигаемая в принципе, в частности разделяемые ресурсы для ОС Windows 95/98 управляются пользователем, даже не системным администратором). Другими словами, с использованием рассмотренной системы не может быть обеспечена централизация управления информационной безопасностью сложной системы, как следствие, снижается ее защищенность (администраторы соответствующих уровней иерархии имеют возможность управлять безопасностью на своих уровнях бесконтрольно со стороны администратора безопасности).

Целью изобретения является повышение уровня защищенности рабочих станций и серверов за счет реализации централизованной системы администрирования информационной безопасностью сложной иерархической информационной системой.

Достигается это тем, что в систему контроля доступа к информационным ресурсам, содержащую блок авторизации пользователя, блок разграничения прав доступа, блок хранения прав доступа, причем первый вход/выход блока авторизации пользователя соединен со входом/выходом авторизации пользователя, второй вход/выход – с первым входом/выходом блока хранения прав доступа, второй вход/выход которого – со входом/выходом блока разграничения прав доступа, первый вход которого – с выходом блока авторизации пользователя, второй вход – со входом запроса доступа, второй выход – с первым входом блока хранения прав доступа, второй вход которого – со входом задания параметров доступа, дополнительно введены: блок авторизации администратора безопасности, блок таймера, блок добавочного разграничения прав доступа, блок хранения эталонных настроек

ек прав доступа, блок сравнения прав доступа с эталоном, блок формирования и восстановления текущих прав доступа, причем первый вход/выход блока авторизации администратора безопасности соединен со входом/выходом авторизации администратора безопасности, второй вход/выход – с первым входом/выходом блока хранения эталонных настроек, второй вход/выход которого – со входом/выходом блока добавочного разграничения прав доступа, первый вход которого – с первым выходом блока разграничения прав доступа, второй вход – с выходом блока авторизации администратора безопасности, третий вход – со входом запроса доступа администратором безопасности, второй выход – с третьим входом блока хранения эталонных настроек прав доступа, второй вход которого – с выходом блока хранения прав доступа, с первым входом блока сравнения прав доступа с эталоном, с первым входом блока формирования и восстановления текущих прав доступа, первый вход – со входом формирования эталонных настроек, с четвертым входом блока хранения прав доступа, с третьим входом блока сравнения прав доступа с эталоном, четвертый вход – со входом задания эталонных настроек, пятый вход – с выходом блока таймера, с пятым входом блока разграничения прав доступа, выход – со вторым входом блока сравнения прав доступа с эталоном, с третьим входом блока формирования и восстановления текущих прав доступа, второй вход которого – с выходом блока сравнения прав доступа с эталоном, выход – с третьим входом блока разграничения прав доступа, первый выход блока добавочного разграничения прав доступа – с выходом разрешения доступа, первый вход блока таймера – со входом задания режима таймера, второй вход – со входом запуска/останова таймера.

Схема системы контроля доступа к информационным ресурсам приведена на фиг. 2, она содержит: блок авторизации пользователя 1, блок авторизации администратора безопасности 2, блок таймера 3, блок разграничения прав доступа 4, блок хранения прав доступа 5, блок хранения эталонных настроек прав доступа 6, блок добавочного разграничения прав доступа 7, блок сравнения прав доступа с эталоном 8, блок формирования и восстановления текущих прав доступа 9, причем первый вход/выход блока авторизации пользователя 1 соединен со входом/выходом авторизации пользователя 10, второй вход/выход – с первым входом/выходом блока хранения прав доступа 5, второй вход/выход которого – со входом/выходом блока разграничения прав доступа 4, первый вход которого – с выходом блока авторизации пользователя 1, второй вход – со входом запроса доступа 11, второй выход – с первым входом блока хранения прав доступа 5, второй вход которого – со входом задания параметров доступа 12, первый вход/выход блока авторизации администратора безопасности 2 соединен со входом/выходом авторизации администратора безопасности 13, второй вход/выход – с первым входом/выходом блока хранения эталонных настроек 6, второй вход/выход которого – со входом/выходом блока добавочного разграничения прав доступа 7, первый вход которого – с первым выходом блока разграничения прав доступа 4, второй вход – с выходом блока авторизации администратора безопасности 2, третий вход – со входом запроса доступа администратором безопасности 18, второй выход – с третьим входом блока хранения эталонных настроек прав доступа 6, вто-

рой вход которого – с выходом блока хранения прав доступа 5, с первым входом блока сравнения прав доступа с эталоном 8, с первым входом блока формирования и восстановления текущих прав доступа 9, первый вход – со входом формирования эталонных настроек 15, с четвертым входом блока хранения прав доступа 5, с третьим входом блока сравнения прав доступа с эталоном 8, четвертый вход – со входом задания эталонных настроек 14, пятый вход – с выходом блока таймера 3, с пятым входом блока разграничения прав доступа 5, выход – со вторым входом блока сравнения прав доступа с эталоном 8, с третьим входом блока формирования и восстановления текущих прав доступа 9, второй вход которого – с выходом блока сравнения прав доступа с эталоном 8, выход – с третьим входом блока разграничения прав доступа 5, первый выход блока добавочного разграничения прав доступа 7 – с выходом разрешения доступа 19, первый вход блока таймера 3 – со входом задания режима таймера 16, второй вход – со входом запуска/останова таймера 17.

Работает система следующим образом. Перед началом работы пользователь должен пройти авторизацию со входа 10, которая осуществляется блоком 1, параметры авторизации – имя и пароль пользователя блок 1 запрашивает и получает от блока 5. Данные текущего пользователя блоком 1 выдаются в блок 4, которым запрашиваются в блоке 5 таблица разграничения прав доступа, зарегистрированного в системе пользователя. При запросе пользователем доступа к информационным ресурсам со входа 11 (запрашивается объект доступа, например, файл и действия, например, чтение или запись) блок 4 анализирует заданные для пользователя права доступа и запрашиваемые пользователем параметры доступа, если они не противоречивы – запрашиваемый доступ системой разрешен, вырабатывается сигнал разрешения доступа к информационному ресурсу, который поступает в блок 7. Со входа 12 задаются параметры прав доступа, изменять данные права разрешается пользователю, имеющему соответствующие полномочия (в зависимости от иерархического уровня системы это может быть как собственно пользователь, так и один из администраторов: системный, СУБД, приложения) – если выдается соответствующий сигнал со второго выхода блока 4, формируемый после авторизации пользователя и его запроса (со входа 11) на получение доступа к блоку 5 (блок 5 в общем случае также является файловым объектом). Аналогично работает схема авторизации и разграничения доступа администратора безопасности. Перед началом работы администратор безопасности должен пройти авторизацию со входа 13, которая осуществляется блоком 2, параметры авторизации – имя и пароль администратора безопасности блок 2 запрашивает и получает от блока 6. Данные текущего пользователя (администратора безопасности) блоком 2 выдаются в блок 7, которым запрашиваются в блоке 6 таблица разграничения прав доступа, зарегистрированного в системе пользователя (администратора безопасности). При запросе пользователем (администратором безопасности) доступа к информационным ресурсам со входа 18 (запрашивается объект доступа, например, файл и действия, например, чтение или запись, способ задания эталонной таблицы настроек) блок 7 анализирует заданные для пользователя права доступа и запрашиваемые пользователем параметры доступа, если они не противоречивы –

запрашиваемый доступ системой разрешен, вырабатывается сигнал разрешения доступа к блоку 6. Со входов 14, либо 15 задаются параметры прав доступа, изменять данные права разрешается пользователю (администратору безопасности), имеющему соответствующие полномочия – если выдается соответствующий сигнал со второго выхода блока 7, формируемый после авторизации пользователя (администратора безопасности) и его запроса (со входа 18) на получение доступа к блоку 6 (блок 6 в общем случае также является файловым объектом) Таким образом, блоки 1, 4, 5 служат для контроля доступа пользователей к файловым объектам, их администрирование осуществляется пользователем, либо соответствующим администратором (системным, СУБД, приложений). Администратор безопасности, пройдя авторизацию в блоке 2 в рамках своих полномочий (его доступ разграничивается блоком 7) создает в блоке 6 эталонные настройки, либо ограничения на настройки разграничений, заданных в блоке 5. Создание эталонных настроек предполагает, что администратором безопасности в блоке 6 задается таблица разграничений доступа, являющаяся эталоном для блока 5. Администратор безопасности имеет две возможности задания таких настроек, либо занесением их в блок 6 со входа 14 самостоятельно (например, с клавиатуры), либо копированием их из блока 5. При этом администратором выдается сигнал на вход 15, по которому настройки из блока 5 перезаписываются в блок 6, работа блока 8 на это время блокируется. Другой режим – это задание ограничений на возможные в блоке 5 настройки. Например, разрешить пользователю для разделения только какой-либо диск, каталог, файл, либо, наоборот, запретить пользователю для разделения диск, каталог, файл и т. д. Данные ограничения также в блок 6 выдаются со входа 14 после обработки соответствующего запроса администратора безопасности со входа 18 (соответственно, происходит авторизация администратора и контролируется его доступ блоком 7). Итак, администратором безопасности в блоке 6 создаются (с клавиатуры – со входа 14, либо копированием из блока 5 – со входа 15) эталонные настройки, либо ограничения на разграничения прав доступа, в соответствии с которыми должен обрабатываться доступ пользователей к информационным ресурсам со входа 11. Далее администратором безопасности со входа 16 задается режим контроля настроек (интервал выдачи сигналов контроля таймером) и со входа 3 запускается таймер – блок 3. Сигналами с выхода блока 3 в блок 8 с выхода блока 5 и с выхода блока 6 заносятся текущие параметры разграничения доступа (из блока 5) и эталонные настройки, либо ограничения (с блока 6). Блок 8 осуществляет сравнение текущих и эталонных настроек, либо выполнение текущими настройками ограничений, задаваемых в блоке 6. При обнаружении некорректности текущих настроек, блок 8 выдает об этом сигнал в блок 9, который, получая текущие настройки из блока 5 и эталонные настройки, либо ограничения на настройки из блока 6, корректирует текущие настройки в соответствии с разграничениями, задаваемыми администратором безопасности, и заносит их в блок 5 на место некорректных текущих настроек. При занесении настроек в блок 6 таймер (блок таймера 3) отключается со входа 17. Ввиду того, что блок 6 также представляет собой файловый объект, разрешение доступа пользователя к информационному ресурсу с первого выхода блока 4 походит дополнительное разграничение на блоке 7

(блок 7 запрещает корректировку информации в блоке 6 всем, кроме администратора безопасности). В случае корректного запроса доступа пользователем, блоком 7 вырабатывается сигнал на выход 19.

Таким образом, заявляемая система позволяет реализовать различные уровни компромисса в централизации администрирования информационной безопасностью в иерархической информационной системе.

Возможны следующие режимы функционирования системы: 1. Все управление безопасностью осуществляется администратором безопасности. В этом случае он самостоятельно (со входа 14) заносит в блок 6 эталонные настройки доступа. После этого запускает таймер (блок 3) со входа 17. Система переходит в режим контроля текущих настроек разграничения доступа в блоке 5 – заносит туда настройки из блока 6 при первом обнаружении несовпадения, фиксируемом блоком 8. При этом любые изменения настроек блока 5, вносимые пользователем, либо администратором соответствующего уровня иерархии системы после их соответствующей авторизации блоком 1 в рамках разграничений, задаваемых блоком 5 (системным администратором, администратором СУБД, администратором приложения), с интервалом времени, задаваемым со входа 16, будут восстановлены. При незначительном интервале данные настройки не успеют вступить в действие.

2. Администратором безопасности решаются задачи контроля и противодействия несанкционированному изменению настроек безопасности. В этом режиме администратор безопасности, после соответствующего визуального контроля настроек, заданных пользователем, либо соответствующим администратором, в блоке 5, переносит данные настройки сигналом со входа 15 в блок 6 – эти настройки считаются корректными (эталонными). Затем запускает подсистему контроля настроек, запустив блок таймера 3 со входа 17. Система переходит в режим контроля, при котором без участия администратора безопасности невозможно изменить настройки разграничения доступа к информационным ресурсам, хранящиеся в блоке 5, в том числе и легальным пользователем, либо администратором в рамках разграничений, задаваемых блоками 1 и 4 (т.е. любые изменения, проводимые без ведома администратора безопасности будут немедленно устранены). Для изменения эталонных настроек необходимо отключить блок таймера 3 (со входа 17), изменить настройки таблицы разграничений прав доступа в блоке 5 (соответствующим пользователем или администратором, в рамках полномочий, заданных блоками 1 и 4, в случае необходимости, при визуальном контроле со стороны администратора безопасности) администратором безопасности, после его (блоком 2) со входа 15 переписать в блок 6 новые корректные настройки. Затем запускается блок 3, система переходит в штатный режим.

3. Администратором безопасности вносятся ограничения на возможности задания параметров безопасности. В этом режиме предполагается, что администратором безопасности в блоке 6 задаются не эталонные таблицы настроек для блока 5, а ограничения на настройки. Возможны два режима ограничений – запреты и разрешение. При реализации режима запретов, вносятся запреты на какие-либо действия, связанные с доступом к информационным ресурсам, например, запретить доступ к какому-нибудь файловому объекту, запретить возможность раз-

деления какого-либо ресурса (например, создать общую папку) запретить доступ к файловому объекту на запись и т. д. То есть данный режим реализует правило, все, что не запрещено администратором безопасности – разрешено в системе. Другой режим реализует альтернативное правило – все, что не разрешено администратором безопасности, запрещено в системе. В этом случае администратором безопасности задаются разрешения, в рамках которых уже может осуществлять свои разграничения пользователь или иной администратор. Например, администратор безопасности может разрешить доступ только к одному логическому диску. Уже к каталогам и файлам, расположенным на этом диске, может разграничивать доступ соответствующий пользователь или администратор со входа 12. В данном режиме ограничения заносятся администратором безопасности (после его авторизации блоком 2) в блок 6, после чего со входа 17 запускается блок таймера 3. Текущие настройки, расположенные в блоке 5, и ограничения из блока 6 с интервалом, заданным со входа 16, поступают в блок 8, который анализирует, не противоречат ли настройки в блоке 5 ограничениям, задаваемым блоком 6. Если противоречат, то блок 9 осуществляет их корректировку и заносит в блок 5 корректные настройки.

Иллюстрация использования заявляемой системы в иерархической информационной системе приведена на фиг.3. Здесь выделены три уровня иерархии информационной системы – системный (ОС), СУБД, приложения, каждый из которых управляется соответствующим администратором. В систему устанавливается заявляемая система контроля доступа к информационным ресурсам (СКД к ИР), управляемая администратором безопасности. Каждый уровень иерархии системы имеет свою систему контроля доступа (прототип) к информационным ресурсам. Настройки всех этих систем в одном из трех, рассмотренных выше режимов, ставятся на контроль администратором безопасности. Это позволяет реализовать в иерархической информационной системе схему централизованного администрирования информационной безопасностью с выделением в качестве структурообразующего элемента данной схемы – администратора безопасности. В качестве замечания отметим, что функции администратора безопасности могут быть совмещены с функциями системного администратора.

Отличие использования системы с различными объектами – системный уровень, СУБД, приложения, состоит в реализации блоков 5 и 6, доступа к ним, способов чтения и записи информации. Для СУБД – это служебные таблицы, размещаемые в файле, для системного уровня и приложений это могут быть различные файлы (например, реестр, для ОС Windows). Чтение и запись информации для данных блоков осуществляется соответственным системным средством – ОС или СУБД.

Блоки, используемые в заявляемой системе, могут быть реализованы следующим образом.

Блоки 2, 6, 7 реализованы аналогично соответствующим блокам 1, 5, 4 прототипа (единственное отличие блока 6 от блока 5 состоит в том, что он содержит как учетные параметры доступа администратора безопасности – данные авторизации и разграничения доступа, так и эталонные настройки, либо ограничения).

Блок 3 – это таймер, программным образом вырабатывающий меандр сигналов задаваемой частоты.

Блок 8 – это программное средство сравнения таблиц (таблицы текущих разграничений с эталоном, либо текущей таблицы разграничений с заданными ограничениями).

Блок 9 – это программное средство формирования корректной таблицы разграничений по результатам сравнения (несовпадением) текущей таблицы с эталонной – за основу берется эталонная, либо с ограничениями – удаляются или заменяются строки таблицы, некорректные с точки зрения заданных ограничений.

Таким образом, реализация всех используемых блоков достигается стандартными средствами, базирующимися на классических основах вычислительной техники.

К достоинствам предлагаемой системы может быть отнесено следующее.

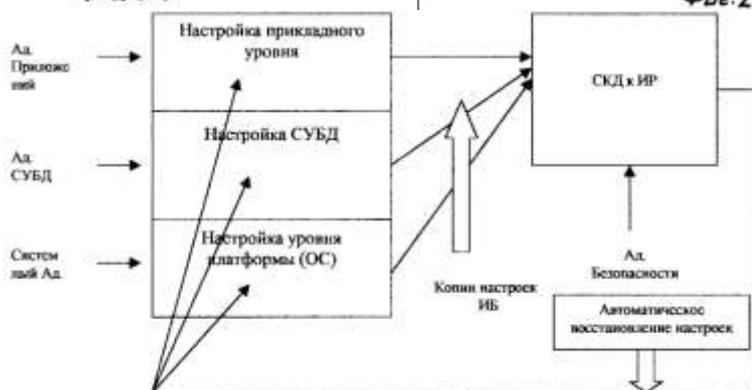
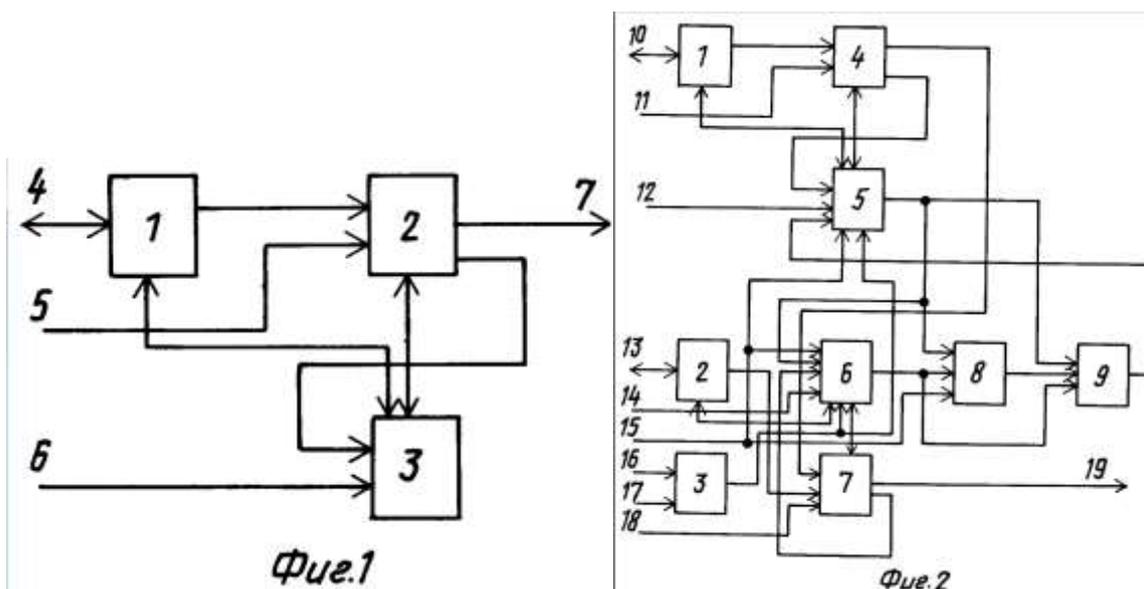
1. Система позволяет реализовать централизованную схему администрирования информационной безопасностью иерархической информационной системы с использованием в качестве структурообразующего звена данной схемы выделенного администратора безопасности.

2. Система позволяет реализовать различные варианты централизации решения задачи администрирования информационной безопасностью – с возложением на администратора безопасности всей совокупности задач администрирования, задач по контролю и противодействию несанкционированному изменению настроек безопасности иными администраторами и пользователями системы, задач по заданию ограничений на возможности осуществления настроек информационной безопасности иными администраторами и пользователями системы.

Формула изобретения

Система контроля доступа к информационным ресурсам, содержащая блок авторизации пользователя, блок разграничения прав доступа, блок хранения прав доступа, причем первый вход/выход блока авторизации пользователя соединен со входом/выходом авторизации пользователя системы, второй вход/выход – с первым входом/выходом блока хранения прав доступа, второй вход/выход которого – со входом/выходом блока разграничения прав доступа, первый вход которого соединен с выходом блока авторизации пользователя, второй вход – со входом запроса доступа системы, второй выход – с первым входом блока хранения прав доступа, второй вход которого соединен со входом задания параметров доступа системы, отличающаяся тем, что дополнительно введены блок авторизации администратора безопасности, блок таймера, блок добавочного разграничения прав доступа, блок хранения эталонных настроек прав доступа, блок сравнения прав доступа с эталоном, блок формирования и восстановления текущих прав доступа, причем первый вход/выход блока авторизации администратора безопасности соединен со входом/выходом авторизации администратора безопасности системы, второй вход/выход – с первым входом/выходом блока хранения эталонных настроек, второй вход/выход которого соединен со входом/выходом блока добавочного разграничения прав доступа, первый вход которого соединен с первым выходом блока разграничения прав доступа, второй вход – с выходом блока авто-

ризации администратора безопасности, третий вход – со входом запроса доступа администратором безопасности системы, второй выход – с третьим входом блока хранения эталонных настроек прав доступа, второй вход которого соединен с выходом блока хранения прав доступа, с первым входом блока сравнения прав доступа с эталоном, с первым входом блока формирования и восстановления текущих прав доступа, первый вход – со входом формирования эталонных настроек системы, с четвертым входом блока хранения прав доступа, с третьим входом блока сравнения прав доступа с эталоном, четвертый вход – со входом задания эталонных настроек системы, пятый вход – с выходом блока таймера, с пятым входом блока хранения прав доступа, выход – со вторым входом блока сравнения прав доступа с эталоном, с третьим входом блока формирования и восстановления текущих прав доступа, второй вход которого соединен с выходом блока сравнения прав доступа с эталоном, выход – с третьим входом блока хранения прав доступа, первый выход блока добавочного разграничения прав доступа – с выходом разрешения доступа системы, первый вход блока таймера – со входом задания режима таймера системы, второй вход – со входом запуска/останова таймера системы<sup>1</sup>.



Фиг. 3

### Подсистема регистрации и учета

Подсистема регистрации и учета предназначена для регистрации в системном журнале, представляющем собой специальный файл, размещаемый на жестком диске ПЭВМ, различных событий, происходящих при работе ПЭВМ. При регистрации событий в системном журнале регистрируются:

- дата и время события;
- имя и идентификатор пользователя, осуществляющего регистрируемое действие;
- действия пользователя (сведения о входе/выходе пользователя в/из системы, запусках программ, событиях НСД, изменении полномочий и др.). Доступ к системному журналу возможен только администратору ИБ (супервизору). События, регистрируемые в системном журнале, определяются администратором СЗИ.

Эта подсистема также реализует механизм обнуления освобождаемых областей памяти.

### **Подсистема контроля целостности.**

Подсистема обеспечения целостности предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) программной и аппаратной среды ПЭВМ, в том числе программных средств комплекса и обрабатываемой информации, обеспечивая при этом защиту ПЭВМ от внедрения программных закладок и вирусов. В программно-аппаратных комплексах систем защиты информации (ПАКСЗИ) от НСД это обычно реализуется:

- проверкой уникальных идентификаторов аппаратных частей ПЭВМ;
- проверкой целостности назначенных для контроля системных файлов, в том числе файлов ПАКСЗИ НСД, пользовательских программ и данных;
- контролем обращения к операционной системе напрямую, в обход прерываний DOS;
- исключением возможности использования ПЭВМ без аппаратного контроллера комплекса;
- механизмом создания замкнутой программной среды, запрещающей запуск привнесенных программ, исключающих несанкционированный выход в ОС.

При проверке целостности программной среды ПЭВМ вычисляется контрольная сумма файлов и сравнивается с эталонным (контрольным) значением, хранящимся в специальной области данных. Эти данные заносятся при регистрации пользователя и могут изменяться в процессе эксплуатации ПЭВМ. В комплексах защиты от НСД используется сложный алгоритм расчета контрольных сумм -вычисление значения их хэш-функций, исключающий факт необнаружения модификации файла.

## Подсистема криптографической защиты.

Подсистема криптографической защиты предназначена для усиления защиты пользовательской информации, хранящейся на жестком диске ПЭВМ или сменных носителях. Подсистема криптографической защиты информации позволяет пользователю зашифровать/расшифровать свои данные с использованием индивидуальных ключей, как правило, хранящихся в персональном ТМ-идентификаторе.

## Межсетевое экранирование.

**Межсетевой экран** или брандмауэр (firewall) – программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивающая защиту информационной системы посредством фильтрации информации.

### Второстепенные термины

- Классификация межсетевых экранов.
- Характеристика межсетевых экранов.

### Структурная схема терминов



Одним из эффективных механизмов обеспечения информационной безопасности распределенных вычислительных сетей является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware, следует принимать во внимание протокол SPX/IPX.

### **Характеристика межсетевых экранов**

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Типы межсетевых экранов и уровни модели ISO OSI

№	Уровень модели OSI	Протокол	Тип межсетевого экрана
1	Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	Шлюз прикладного уровня; Межсетевой экран экспертного уровня.
2	Представления данных		
3	Сеансовый	TCP, UDP	Шлюз сеансового уровня
4	Транспортный	TCP, UDP	
5	Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
6	Канальный		
7	Физический		

**Межсетевые экраны с фильтрацией пакетов** представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем

анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их с сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

**Шлюзы сеансового уровня** контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функции трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым, исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

**Шлюзы прикладного уровня** проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип меж сетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернет при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что, теоретически, должно обеспечить более эффективную фильтрацию пакетов.

## **Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации.**

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

Современная криптография включает в себя четыре крупных раздела:

1. *Симметричные криптосистемы.* В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. (Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный);

2. *Криптосистемы с открытым ключом.* В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения. (Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.);

3. *Электронная подпись.* Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

4. *Управление ключами.* Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

### **Требования к криптосистемам**

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно

большой стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

### **Симметричные криптосистемы**

Все многообразие существующих криптографических методов в симметричных криптосистемах можно свести к следующим 4 классам преобразований:

- подстановка – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом;
- перестановка – символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;
- аналитическое преобразование – шифруемый текст преобразуется по некоторому аналитическому правилу, например гаммирование – заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа;
- комбинированное преобразование – представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем «чистые» преобразования того или иного класса

в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе.

### **Системы с открытым ключом**

Как бы ни были сложны и надежны криптографические системы – их слабое мест при практической реализации – проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. То есть в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы. Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом. Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату. Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении  $x$  относительно просто вычислить значение  $f(x)$ , однако если  $y = f(x)$ , то нет простого пути для вычисления значения  $x$ . Множество классов необратимых функций порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС. В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени. Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем. Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- Разложение больших чисел на простые множители;
- Вычисление логарифма в конечном поле;
- Вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в следующих назначениях:

1. Как самостоятельные средства защиты передаваемых и хранимых данных.
2. Как средства для распределения ключей.

Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками. Один из наиболее распространенных – система с открытым ключом – RSA. Криптосистема RSA, разработанная в 1977 году и получила название в честь ее создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана. Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время. Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

### **Электронная подпись**

**В** чем состоит проблема аутентификации данных? В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие обычно преследует две цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т. д. Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами – техническая деталь, то с подписью электронной дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправления в документ сможет любой пользователь. С широким распространением в современном мире электронных форм документов (в том числе и конфиденциальных) и средств их обработки особо актуальной стала проблема установления подлинности и авторства безбумажной документации. В разделе криптографических систем с открытым ключом было показано, что при всех преимуществах современных систем шифрования они не позволяют обеспечить аутентификацию данных. Поэтому средства аутентификации должны использоваться в комплексе и криптографическими алгоритмами.

### **Управление ключами**

Кроме выбора подходящей для конкретной ИС криптографической системы, важная проблема – управление ключами. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения кон-

фиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в ИС, где количество пользователей составляет десятки и сотни управление ключами – серьезная проблема. Под ключевой информацией понимается совокупность всех действующих в ИС ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то завладев ею, злоумышленник получает неограниченный доступ ко всей информации. Управление ключами – информационный процесс, включающий в себя три элемента:

- генерацию ключей;
- накопление ключей;
- распределение ключей.

Рассмотрим, как они должны быть реализованы для того, чтобы обеспечить безопасность ключевой информации в ИС.

### **Генерация ключей**

В самом начале разговора о криптографических методах было сказано, что не стоит использовать неслучайные ключи с целью легкости их запоминания. В серьезных ИС используются специальные аппаратные и программные методы генерации случайных ключей. Как правило используют датчики ПСЧ. Однако степень случайности их генерации должна быть достаточно высоким. Идеальными генераторами являются устройства на основе «натуральных» случайных процессов. Например, случайным математическим объектом являются десятичные знаки иррациональных чисел, которые вычисляются с помощью стандартных математических методов.

### **Накопление ключей**

Под накоплением ключей понимается организация их хранения, учета и удаления. Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание. Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован. В достаточно сложной ИС один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей. Итак, каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию называются мастер-ключами. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть, и не хранил их вообще на каких-либо материальных носителях. Очень важным условием безопасности информации является периодическое обновление ключевой информации в ИС. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных ИС обновление ключевой информации желательно делать ежедневно. Вопрос обновления ключевой информации связан и с третьим элементом управления ключами – распределением ключей.

### **Распределение ключей**

Распределение ключей – самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

- Оперативность и точность распределения;
- Скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения ключей отпадает. Тем не менее распределение ключевой информации в ИС требует новых эффективных решений. Распределение ключей между пользователями реализуются двумя разными подходами:

1. Путем создания одного или нескольких центров распределения ключей. Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены и это позволяет читать все сообщения, циркулирующие в ИС. Возможные злоупотребления существенно влияют на защиту.

2. Прямой обмен ключами между пользователями информационной системы. В этом случае проблема состоит в том, чтобы надежно удостоверить подлинность субъектов. Для обмена ключами можно использовать криптосистемы с открытым ключом, используя тот же алгоритм RSA.

В качестве обобщения сказанного о распределении ключей следует сказать следующее. Задача управления ключами сводится к поиску такого протокола распределения ключей, который обеспечивал бы:

- возможность отказа от центра распределения ключей;
- взаимное подтверждение подлинности участников сеанса;
- подтверждение достоверности сеанса механизмом запроса-ответа, использование для этого программных или аппаратных средств;
- использование при обмене ключами минимального числа сообщений.

### **Реализация криптографических методов**

Проблема реализации методов защиты информации имеет два аспекта:

- разработку средств, реализующих криптографические алгоритмы;
- методику использования этих средств.

Каждый из рассмотренных криптографических методов могут быть реализованы либо программным, либо аппаратным способом. Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры. При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы. Большинство зарубежных серийных средств шифрования основано на американском стандарте DES. Отечественные же разработки, такие как, например, устройство КРИПТОН, использует отечественный стандарт шифрования. Основным достоинством программных методов реализации защиты является их гибкость, т. е. возможность быстрого изменения алгоритмов шифрования. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз). В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный «криптографический сопроцессор» – вычислительное устройство, ориен-

тированное на выполнение криптографических операций (сложение по модулю, сдвиг и т. д.). Меняя программное обеспечение для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

Таким образом, выбор типа реализации криптозащиты для конкретной ИС в существенной мере зависит от ее особенностей и должен опираться на всесторонний анализ требований, предъявляемых к системе защиты информации.

### **Идентификация и аутентификация**

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

Идентификация позволяет субъекту – пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова «аутентификация» иногда используют сочетание «проверка подлинности». Субъект может подтвердить свою подлинность, если предъявит 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 или иное устройство аналогичного назначения;
- нечто, что является частью его самого: голос, отпечатки пальцев и т. п., то есть свои биометрические характеристики;
- нечто, ассоциированное с ним, например координаты.

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. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть. Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Пароли уязвимы по отношению к электронному перехвату – это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход – использование криптографии для шифрования паролей перед передачей по линиям связи.

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т. п.);

- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;
- обучение и воспитание пользователей;
- использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации, основанные, например, на применении токенов.

Токен – это предмет или устройство, владение которым подтверждает подлинность пользователя. Различают токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию) и интеллектуальные токены (активные).

Самой распространенной разновидностью токенов с памятью являются карточки с магнитной полосой. Для использования подобных токенов необходимо устройство чтения, снабженное также клавиатурой и процессором. Обычно пользователь набирает на этой клавиатуре свой личный идентификационный номер, после чего процессор проверяет его совпадение с тем, что записано на карточке, а также подлинность самой карточки. Таким образом, здесь фактически применяется комбинация двух способов защиты, что существенно затрудняет действия злоумышленника.

Необходима обработка аутентификационной информации самим устройством чтения, без передачи в компьютер – это исключает возможность электронного перехвата.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

Как известно, одним из самых мощных средств в руках злоумышленника является изменение программы аутентификации, при котором пароли не только проверяются, но и запоминаются для последующего несанкционированного использования.

Интеллектуальные токены характеризуются наличием собственной вычислительной мощности. Они подразделяются на интеллектуальные карты, стандартизованные ISO и прочие токены. Карты нуждаются в интерфейсном устройстве, прочие токены обычно обладают ручным интерфейсом (дисплеем и клавиатурой) и по внешнему виду напоминают калькуляторы. Чтобы токен начал работать, пользователь должен ввести свой личный идентификационный номер.

По принципу действия интеллектуальные токены можно разделить на следующие категории:

- Статический обмен паролями: пользователь обычным образом доказывает токену свою подлинность, затем токен проверяется компьютерной системой;
- Динамическая генерация паролей: токен генерирует пароли, периодически изменяя их. Компьютерная система должна иметь синхронизированный гене-

ратор паролей. Информация от токена поступает по электронному интерфейсу или набирается пользователем на клавиатуре терминала;

- Запросно-ответные системы: компьютер выдает случайное число, которое преобразуется криптографическим механизмом, встроенным в токен, после чего результат возвращается в компьютер для проверки. Здесь также возможно использование электронного или ручного интерфейса. В последнем случае пользователь читает запрос с экрана терминала, набирает его на клавиатуре токена (возможно, в это время вводится и личный номер), а на дисплее токена видит ответ и переносит его на клавиатуру терминала.

### **Управление доступом**

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты – пользователи и процессы могут выполнять над объектами – информацией и другими компьютерными ресурсами. Речь идет о логическом управлении доступом, который реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей. Задача логического управления доступом состоит в том, чтобы для каждой пары (субъект, объект) определить множество допустимых операций, зависящее от некоторых дополнительных условий, и контролировать выполнение установленного порядка. Простой пример реализации таких прав доступа – какой-то пользователь (субъект) вошедший в информационную систему получил право доступа на чтение информации с какого-то диска (объект), право доступа на модификацию данных в каком-то каталоге (объект) и отсутствие всяких прав доступа к остальным ресурсам информационной системы.

Контроль прав доступа производится разными компонентами программной среды – ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением (таким как монитор транзакций) и т. д.

### **Протоколирование и аудит**

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. Например – кто и когда пытался войти в систему, чем завершилась эта попытка, кто и какими информационными ресурсами пользовался, какие и кем модифицировались информационные ресурсы и много других.

Аудит – это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие главные цели:

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

### **Виртуальные частные сети.**

**Услуга IP VPN** – услуга построения частных виртуальных сетей (**VPN**) по технологии IP. Предназначены для корпоративных пользователей имеющих несколько офисов с локальными сетями и желающих объединить данные сети в единое информационное пространство без построения собственных цифровых линий связи между каждым из этих локальных сетей для создания распределенной корпоративной сети.

Приобретая услуги **VPN**, пользователь услуг получает на территории центрального федерального округа следующие возможности:

- организовать высококачественную видеоконференцсвязь,
- организовать передачу любой корпоративной информации, в том числе электронной почты, передачу файлов, доступ к базам данных в реальном масштабе времени;
- организовать передачу цифровых потоков.

Инфраструктура **VPN** абонента создается на базе сети передачи данных Филиала и мультисервисной магистральной сети передачи данных IP/MPLS (МСПД) ОАО «Ростелеком».

Подключение к организованной виртуальной частной сети (далее «**VPN-сеть**») осуществляется на основе технологий, применяющихся в КФ ОАО «Ростелеком», для организации каналов передачи данных.

**VPN** сеть пользователя отделена от публичных сетей Интернет и других **VPN** сетей на уровне маршрутизации, то есть трафик пользователя защищен от несанкционированного доступа извне. Передача информации на канале доступа к **VPN**-сети осуществляется на скоростях не выше скорости передачи данных, обеспечиваемой оборудованием «последней мили».

### **Преимущества пользовательских VPN**

Пользовательские **VPN** обладают двумя основными преимуществами:

- Сотрудники, находящиеся в командировке, могут осуществлять доступ к электронной почте, файлам и внутренним системам в любое время без необходимости в осуществлении дорогостоящих междугородних и международных телефонных вызовов для соединения с серверами.
- Сотрудники, работающие из дома, могут осуществлять доступ к службам сети, как и сотрудники, работающие в организации, без аренды дорогостоящих выделенных каналов.

Оба эти преимущества можно приписать к экономии денежных средств. Экономия может заключаться в отказе от использования дорогостоящих междугородних и международных соединений, арендуемых каналов связи или в выполнении сотрудниками задач по администрированию серверов, принимающих входящие телефонные соединения. Домашние пользователи с *DSL* или кабельными модемами могут добиться увеличения скорости при использовании линий телефонной связи со скоростями 56 Кбит/с. Все больше гостиничных номеров оборудуются соединениями для доступа в *сеть*, поэтому для пользователей, находящихся в поездке, создаются все условия для высокоскоростного доступа в *сеть*.

## **Проблемы, связанные с пользовательскими VPN**

Правильное использование пользовательских VPN может снизить *затраты* организации, но пользовательские VPN не являются решением всех возможных проблем. При их использовании имеют *место* значительные риски, связанные с безопасностью, и проблемы реализации, с которыми приходится считаться.

Возможно, самой большой проблемой безопасности при использовании VPN сотрудником является одновременное соединение с другими сайтами интернета. Как правило, *программное обеспечение VPN* на компьютере пользователя определяет, должен ли трафик передаваться через VPN, либо его необходимо отправить на какой-либо другой *сайт* в открытом виде. Если на *компьютер* пользователя была произведена *атака* с использованием «*троянского коня*», возможно, что некий внешний нелегальный *пользователь* использует *компьютер* сотрудника для подключения к внутренней сети организации (см. рис. 11.3). Атаки данного типа осуществляются довольно сложно, но они совершенно реальны.

Пользовательские VPN требуют такого же внимания к вопросам, связанным с управлением пользователями, как и внутренние системы. В некоторых случаях пользователи VPN могут быть привязаны к идентификаторам пользователей в домене *Windows NT* или *Windows 2000* или к другой системе централизованного управления пользователями. Эта возможность упрощает управление пользователями, однако администраторам по-прежнему следует сохранять бдительность и следить за тем, каким пользователям требуется удаленный *VPN-доступ*, а каким – нет.

## **Управление пользовательскими VPN**

Управление пользовательскими VPN, главным образом, заключается в управлении пользователями и их компьютерами. При разделении сотрудников необходимо выполнять соответствующие процедуры по управлению пользователями.

Разумеется, на компьютерах пользователей должны устанавливаться правильные версии программного обеспечения VPN и реализовываться соответствующие конфигурации. Если компьютеры принадлежат организации, это *программное обеспечение* является стандартным компонентом для каждого компьютера. Если организация разрешает сотрудникам использовать VPN со своих домашних компьютеров, ей понадобится увеличить общий *уровень поддержки* этих пользователей, так как различные компьютеры и поставщики услуг интернета могут требовать наличие различных конфигураций.

## **Понятие стандартных технологий функционирования VPN**

*Сеть VPN* состоит из четырех ключевых компонентов:

- Сервер VPN.
- Алгоритмы шифрования.
- Система аутентификации.
- Протокол VPN.

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована *архитектура VPN*, зависит от правильности определения требований. *Определение требований* должно включать в себя следующие аспекты.

- Количество времени, в течение которого необходимо обеспечивать защиту информации.
- Число одновременных соединений пользователей.
- Ожидаемые типы соединений пользователей (сотрудники, работающие из дома или находящиеся в поездке).
- Число соединений с удаленным сервером.
- Типы сетей VPN, которым понадобится соединение.
- Ожидаемый объем входящего и исходящего трафика на удаленных узлах.
- Политика безопасности, определяющая настройки безопасности.

При разработке системы также может оказаться полезным указать дополнительные требования, связанные с местоположением сотрудников, находящихся в поездке (имеются в виду узлы в других организациях или в номерах отелей), а также типы служб, которые будут работать через VPN.

### **Сервер VPN**

*Сервер VPN* представляет собой *компьютер*, выступающий в роли конечного узла соединения VPN. Данный *сервер* должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Большая часть производителей программного обеспечения VPN должна предоставлять рекомендации по поводу производительности процессора и конфигурации памяти, в зависимости от числа одновременных VPN-соединений. Следует обеспечить наличие системы с соответствующими параметрами, а также позаботиться о ее дальнейшей модернизации.

### **Алгоритмы шифрования**

*Алгоритм* шифрования, используемый в VPN, должен быть стандартным мощным алгоритмом шифрования (в "Шифрование" приведена более подробная информация о системах шифрования). Возникает вопрос: какая же система шифрования самая лучшая? Вообще, все стандартные и мощные алгоритмы могут эффективно использоваться при построении VPN. Различные производители отдают предпочтение различным алгоритмам, в зависимости от ограничений реализации продукта, аспектов, связанных с лицензированием, и предпочтений по программированию. Приобретая программный пакет VPN, следует выслушать комментарии специалистов и убедиться в том, что производитель использует мощный *алгоритм* шифрования.

Читатель может обратить внимание на то, что в предыдущем абзаце уделено особое внимание выбору алгоритма шифрования. Следует заметить, что выбор алгоритма не имеет принципиального значения, если он будет стандартным и в достаточной степени мощным. Гораздо больше влияет на общий уровень безопасности реализация системы. Неправильно реализованная система может сделать бесполезным самый мощный *алгоритм* шифрования. Приняв во внимание сказанное выше, давайте изучим риски, связанные с использованием VPN. Для того чтобы получить доступ к информации, передаваемой через VPN, злоумышленник должен:

- захватить весь сеанс соединения, т. е. разместить устройство прослушивания между противоположными концами соединения в том месте, через которое должен передаваться весь трафик VPN;

- использовать большие вычислительные мощности и большое количество времени для перехвата ключа с помощью грубой силы и для дешифрования трафика.

Злоумышленнику гораздо проще использовать имеющуюся *уязвимость* на компьютере пользователя либо украсть портативный *компьютер*, например, в аэропорту. Если *информация* не представляет собой особой важности, в *VPN* можно использовать любой широко распространенный, мощный *алгоритм* шифрования.

### **Система аутентификации**

Третьим компонентом архитектуры *VPN* является *система аутентификации*. Как уже говорилось ранее, *система аутентификации VPN* должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. При использовании пользовательских *VPN* отдается предпочтение первым двум вариантам.

Хорошей комбинацией средств аутентификации являются смарт-карты в паре с персональным идентификационным номером или паролем. Производители программного обеспечения, как правило, предоставляют организациям на выбор несколько систем аутентификации. В данном перечне присутствуют ведущие производители смарт-карт.

### **Протокол VPN**

Протокол *VPN* определяет, каким образом система *VPN* взаимодействует с другими системами в интернете, а также уровень защищенности трафика. Если рассматриваемая организация использует *VPN* только для внутреннего информационного обмена, вопрос о взаимодействии можно оставить без внимания. Однако если организация использует *VPN* для соединения с другими организациями, собственные протоколы использовать, скорее всего, не удастся. В разговоре об алгоритме шифрования было упомянуто, что внешние окружающие факторы могут оказывать большее влияние на *безопасность системы*, чем *алгоритм* шифрования. Протокол *VPN* оказывает влияние на общий уровень *безопасности системы*. Причиной этому является тот факт, что протокол *VPN* используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, *злоумышленник* может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества *VPN*.

При соединении рекомендуется использовать *стандартные протоколы*. В настоящее время *стандартным протоколом* для *VPN* является *IPSec*. Этот протокол представляет собой *дополнение* к *IP*, осуществляющее инкапсуляцию и *шифрование* заголовка *TCP* и полезной информации, содержащейся в пакете. *IPSec* также поддерживает обмен ключами, удаленную аутентификацию сайтов и согласование алгоритмов (как алгоритма шифрования, так и хэш-функции). *IPSec* использует *UDP-порт 500* для начального согласования, после чего используется *IP-протокол 50* для всего трафика. Для правильного функционирования *VPN* эти протоколы должны быть разрешены.

## Типы систем VPN

Теперь, после обсуждения функционирования сетей *VPN*, давайте рассмотрим непосредственное применение *VPN* внутри организации. Помимо вопросов, связанных с политикой и управлением, организации нужно выбрать тип приобретаемой системы *VPN*. На момент написания данной книги можно выделить три типа *VPN*-построителей:

- аппаратные системы;
- программные системы;
- веб-системы.

### Аппаратные системы

Аппаратные системы *VPN*, как правило, базируются на аппаратной платформе, используемой в качестве *VPN*-сервера. На этой платформе выполняется *программное обеспечение* производителя, а также, возможно, некоторое специальное *программное обеспечение*, предназначенное для улучшения возможностей шифрования. В большинстве случаев для построения *VPN* на системе удаленного пользователя необходимо наличие соответствующего программного обеспечения. Аппаратные платформы также могут использоваться для построения межузловых *VPN*, хотя это зависит от производителя оборудования.

Аппаратная система *VPN* имеет два преимущества.

- **Скорость.** Оборудование, как правило, оптимизировано для поддержки *VPN*, посредством чего обеспечивается преимущество в скорости по сравнению с компьютерными *системами общего назначения*. За счет этого достигается возможность поддержки большего числа одновременных *VPN*-соединений.
- **Безопасность.** Если аппаратная платформа специально разработана для приложения *VPN*, из ее системы удалены все лишние программы и процессы. За счет этого снижается степень подверженности атакам по сравнению с компьютерной системой общего назначения, в которой работают другие процессы. Это не значит, что компьютер общего назначения не может быть должным образом защищен. Как правило, использование компьютера общего назначения требует дополнительных усилий по настройке безопасности.

### Программные системы

Программные *VPN* работают на компьютерных системах общего назначения. Они могут быть установлены на выделенной для *VPN* системе либо совместно с другим программным обеспечением, таким как *межсетевой экран*. При загрузке программного обеспечения необходимо обеспечить достаточную *мощность* аппаратной платформы для поддержки *VPN*. Так как *VPN*-продукт устанавливается на компьютеры, имеющиеся в организации, руководство организации должно позаботиться о соответствии компьютеров предъявляемым требованиям.

Программные *VPN*-системы могут использоваться таким же образом, как и аппаратные системы. Существует *программное обеспечение* для поддержки пользовательских и узловых *VPN*.

## Веб-системы

Главным недостатком большинства пользовательских систем *VPN* является потребность в установке программного обеспечения на систему-клиент. Бесспорно, что *программное обеспечение*, которое устанавливалось на клиентские системы, увеличивало объем *работ* по управлению пользовательскими *VPN*. Более того, клиентское *программное обеспечение* во многих случаях не работало должным образом с некоторыми приложениями, загруженными на *компьютер-клиент*. Это обстоятельство повышало *стоимость* поддержки и приводило к тому, что многие организации стали устанавливать на специально выделенные компьютеры только *программное обеспечение VPN*.

Указанные проблемы привели к тому, что некоторые производители *VPN* стали рассматривать веб-браузеры в качестве *VPN-клиентов* и реализовывать этот подход на практике. Он заключается в том, что *пользователь* с помощью браузера подключается к *VPN* через *SSL*. *SSL* обеспечивает *шифрование* трафика, а подтверждение подлинности пользователя выполняется с помощью средств аутентификации, встроенных в систему. Для предоставления пользователю необходимых услуг используется несколько различных механизмов. Среди них можно выделить надстройки браузера и виртуальные машины *Java*.

В то время как *стоимость* поддержки и обслуживания несомненно ниже, на момент написания этой книги ни одна из бесклиентных систем *VPN* не обеспечивает полную функциональность. Этим сетям *VPN* присущи ограничения, заключающиеся в наборе используемых приложений и методе подключения пользователей к внутренним системам. Организациям следует рассматривать *вариант использования* таких систем, так как это снижает *затраты* на обслуживание, однако необходимо учитывать непосредственные требования пользователей и согласовать их с ограничениями, имеющимися в системах.

### Определение различий между типами VPN

На предприятии принято решение использовать *VPN*, в результате чего установлен *VPN-построитель*. Необходимо составить оценочный отчет о методах шифрования, протоколах *туннелирования* и аспектах безопасности, связанных с приложениями, которые могут использовать *VPN*, такими как средства передачи голоса и видеоданных через службы *IP* (видеоконференции, усовершенствованные и измененные функции *PBX*) и средства удаленного хранения/резервирования и восстановления. Обязательно ли *шифрование* данных в каждом из случаев?

Для каждого из приложений следует выяснить следующее.

1. Какой тип *VPN* лучше использовать для приложения – межузловую или пользовательскую *VPN*?
2. Где расположены конечные узлы *VPN*? Каким опасностям могут подвергаться эти конечные узлы?
3. Налагают ли конечные узлы или пользователи приложения какие-либо дополнительные требования к механизму аутентификации, связанному с *VPN*?
4. Определите соответствующие приложению механизмы аутентификации.

5. Отследите информацию во время передачи. Является ли она открытой для перехвата или прослушивания? Если да, определите, обеспечивает ли используемый механизм шифрования должный уровень защиты информации.

## 11. Контроль защищенности информации.

### Методы и средства контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН

Существуют две основные методики оценки защищенности технического средства от утечки по каналу ПЭМИН. Это методика специальных исследований, результатом измерения которой является расчет радиусов  $R_2$ ,  $r_1$  и  $r_1'$ , и методика оценки защищенности, результатом которой является измеренное и рассчитанное соотношение сигнал/шум на границе контролируемой зоны (реальное затухание).

В первой методике расчет производится из предположения, что ЭМ-поле распространяется над полупроводящей поверхностью, и применима она соответственно в условиях, близких к этим. Вторая методика учитывает затухание от источника сигнала (в данном случае исследуемого технического средства) до границы контролируемой зоны. Однако в ее рамках не определяются радиусы зоны 1 и зоны 1' и, следовательно, она является заметно более простой. Наиболее объективной является методика определения  $R_2$ ,  $r_1$  и  $r_1'$ , дополненная методом реальных зон.

Зона 2 – минимальное *расстояние* от технического средства, на границе и за пределами которого *отношение* сигнал/шум не превышает нормированного значения. Фактически зона  $R_2$  – это зона, в пределах которой возможен перехват средством разведки ПЭМИН с требуемым качеством.

Если *радиус* Зоны 2 меньше радиуса контролируемой зоны – *информация* считается защищенной. В случае если *радиус* Зоны 2 больше радиуса контролируемой зоны, требуется применять дополнительные меры – *экранирование* или активную защиту, например, генераторы пространственного шума, рассмотренные нами в предыдущих лекциях. Зона 2 для каждого ОТСС определяется инструментально-расчетным методом и, как правило, указывается в эксплуатационной документации.

*Пространство* вокруг технического средства, в пределах которого уровень наведенного от него информативного сигнала в сосредоточенных антеннах превышает допустимое (нормированное) *значение* называется зоной 1 ( $r_1$ ), а в распределенных антеннах – зоной 1' ( $r_1'$ ). В отличие от зоны  $R_2$ , размер зоны  $r_1$  ( $r_1'$ ) зависит не только от уровня побочных электромагнитных излучений, но и от длины случайной антенны (от помещения, в котором установлено техническое средство до места возможного подключения к ней средства разведки).

Зоны  $r_1$  ( $r_1^*$ ) для каждого ОТСС определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия [136].

Методика оценки защищенности по реальному затуханию сводится к измерению соотношения «сигнал-шум» на границе контролируемой зоны и сравнению полученного значения с нормированным.

Для оценки защищенности конфиденциальной информации, обрабатываемой ОТСС от утечки за счет наводок на ВТСС и их коммуникации, выходящие за пределы контролируемой зоны, рассчитывается максимальная *длина* пробега исследуемой линии для каждой из частот, на которой возможно выделение информативного сигнала от ОТСС. Выбирается максимальное из полученных значений и сравнивается с пробегом до границы КЗ. Если *значение* максимального пробега наведенного информативного сигнала больше пробега исследуемой линии до границы КЗ – *информация* недостаточно защищена и требуются дополнительные меры защиты, если меньше – соответственно, *информация* защищена.

В качестве примера средства оценки защищенности ОТСС от утечки информации по каналу ПЭМИН рассмотрим автоматизированную систему «Сигурд».



Автоматизированная система оценки защищенности технических средств от утечки информации по каналу ПЭМИН «Сигурд»

Возможности «Сигурд»:

- автоматизированное исследование технического средства на наличие информативных сигналов ПЭМИН в полном соответствии с действующими нормативно-методическими документами;

- автоматический и ручной поиск сигналов ПЭМИН исследуемого технического средства на фоне постоянно присутствующих радиосигналов по электрической и по магнитной составляющим электромагнитного поля, а также в отходящих линиях;
- автоматическое и ручное распознавание информативных сигналов ПЭМИН;
- расчет показателей защищенности технических средств от утечки информации по каналу ПЭМИН в соответствии с действующими нормативными документами, с выводом результатов по выбору оператора в файл стандарта HTML или MS Word (DOC);
- автоматизированное исследование систем активного зашумления (САЗ) и расчет показателей их эффективности;
- дистанционное автоматическое управление измерительным приемником (анализатором спектра) при поиске сигналов ПЭМИН, а при использовании опции «Сигурд-ИК» – и дистанционное автоматическое управление состоянием исследуемого технического средства при поиске его сигналов ПЭМИН;
- автоматическую передачу исходных данных в расчет показателей защищенности технического средства и эффективности САЗ;
- возможность создания и пополнения базы данных по постоянно присутствующим радиосигналам в выбранном диапазоне частот;
- возможность визуализации в процессе исследования радиосигналов, представляющих интерес;
- формирование сообщений о неверных действиях оператора с указанием характера ошибки;
- расчет минимально допустимых расстояний  $R_2$  от технического средства до границы контролируемой зоны;
- расчет минимально допустимых расстояний  $r_1$  от технического средства до сосредоточенных случайных антенн;
- расчет минимально допустимых расстояний  $r_1'$  от технического средства до распределенных случайных антенн;
- расчет отношения «сигнал/шум» на границе контролируемой зоны;
- расчет отношения «сигнал/шум» на границе контролируемой зоны с учетом применения систем активного зашумления;
- расчет отношения «сигнал/шум» в отходящих линиях;
- расчет отношения «сигнал/шум» в отходящих линиях с учетом применения систем активного зашумления.

### **Методы и средства контроля защищенности акустической речевой информации от утечки по техническим каналам**

Одним из нормированных показателей оценки качества трактов (аппаратуры) телефонной проводной и радиосвязи, в которых используется аналоговый речевой сигнал, является разборчивость речи  $W$ , под которой понимается относи-

тельное количество (в процентах) правильно принятых, переданных по тракту элементов (слогов, слов, фраз) артикуляционных таблиц.

Показатель словесной разборчивости речи используется для оценки эффективности защищенности помещений от утечки речевой информации по акустическому и виброакустическому каналам. Наиболее целесообразно для оценки разборчивости речи использовать инструментально-расчетный метод, основанный на результатах экспериментальных исследований, проведенных Н.Б. Покровским, описанным в книге "Расчет и измерение разборчивости речи". Для оценки разборчивости речи необходимо измерить уровни скрываемого речевого сигнала и шума (помехи) в месте возможного размещения приемных датчиков аппаратуры акустической разведки или в месте возможного прослушивания речи без применения технических средств. При этом считается, что перехват речевой информации возможен, если рассчитанное по результатам измерения значение словесной разборчивости речи  $W$  превышает установленные нормы. Проведенные исследования показали, что с достаточной для инженерных расчетов точностью измерение уровней речевого сигнала и шума необходимо проводить в пяти октавных полосах: 250, 500, 1000, 2000, 4000 Гц.

Таким образом, методика инструментального контроля оценки защищенности акустической речевой информации от утечки по техническим каналам утечки основывается на инструментально-расчетном методе определения отношений «речевой сигнал / акустический (вибрационный) шум» (далее – «сигнал/шум») в контрольных точках в октавных полосах со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц.

Современная аппаратура способна излучать контрольный сигнал одновременно во всех пяти октавных полосах. С учетом того, что *контроль* защищенности требует множественных замеров, это сильно экономит общее время проведения оценки защищенности.

При известном месте расположения источника речевого сигнала (*рабочий стол, место беседы и пр.*) точка установки источника тестовых акустических сигналов располагается в месте расположения источника речевого сигнала. При невозможности определения конкретного месторасположения источника речевого сигнала источник тестовых акустических сигналов располагается на расстоянии 1 м от ближайшей ограждающей конструкции на разведопасном направлении и на таком же расстоянии от других ограждающих конструкций и предметов.

Контрольными точками установки акустического датчика (измерительного микрофона) являются места возможного размещения аппаратуры речевой разведки (стоянки автомобилей, автобусные остановки, скамейки для отдыха, окна близлежащих зданий и т. п.). При невозможности установки измерительного микрофона в реальных местах возможного расположения аппаратуры речевой разведки контрольные точки размещают на границе контролируемой (охраняемой) зоны. При этом в оформлении результатов контроля об этом делается оговорка.

При контроле защищенности речевой информации от виброакустической аппаратуры речевой разведки контрольными точками установки измерительного контактного микрофона (виброакустического датчика) являются внешние по от-

ношению к источнику речевого сигнала поверхности различных ограждающих конструкций, инженерных коммуникаций и других предметов, которые находятся на разведопасных направлениях, а также возможные места на инженерных коммуникациях (строительных конструкциях и т. п.), доступных посторонним лицам.

Рассмотрим пример расположения измерительного оборудования в случае, когда место расположения источника акустических сигналов неизвестно.

Для акустических замеров элементы измерительного комплекса размещаются следующим образом: излучатель тест-сигнала – в 1 метре от конструкции (по нормали к ней) на высоте 1,5 метра от пола, первый микрофон в 0,5 метра от ограждающей конструкции, второй за ней – в 0,5 метра. Если стена сплошная и в ней нет трещин и прочих дефектов, то можно сделать всего пару замеров. Если же есть подозрения на трещины или они видны визуально, необходимо увеличение числа контрольных точек. Максимально контрольные точки располагаются в 1,5–2 м друг от друга. На рисунках показаны варианты размещения датчиков при проведении замеров ограждающих конструкций и окон.

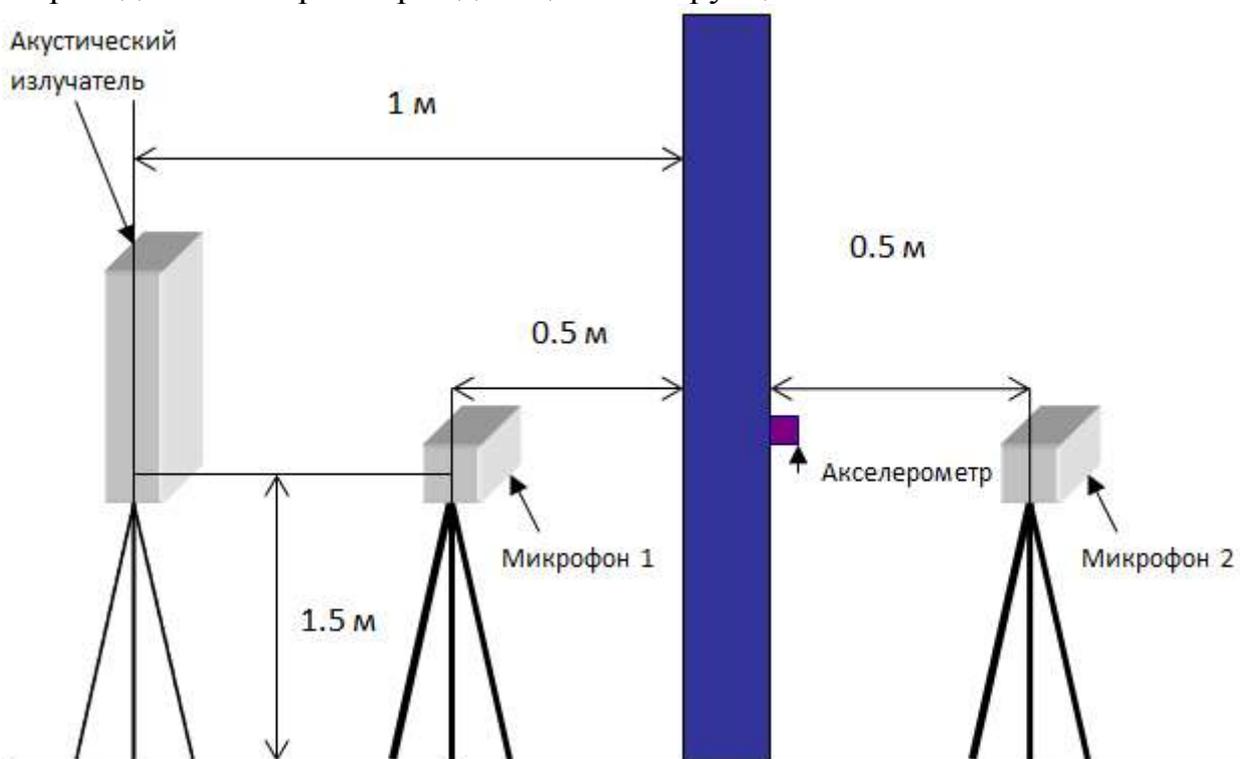


Схема измерения звукоизоляции стены (перегородки)

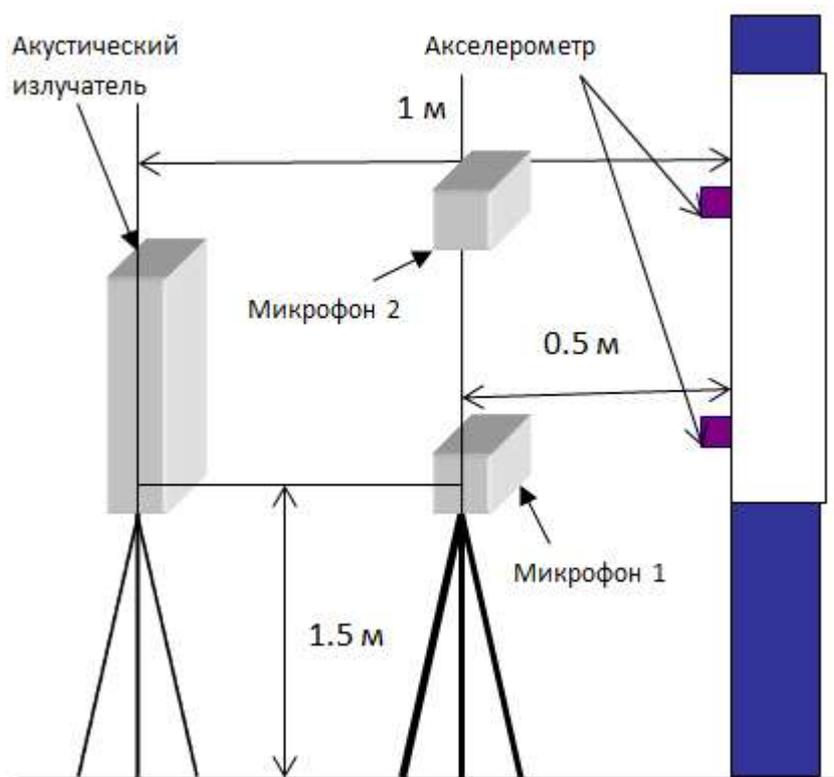


Схема измерения звукоизоляции на окне

Аналогично выполняются измерения по виброакустическому каналу. Важно, что при оценке эффективности защиты информации от утечки по виброакустическим каналам необходимо контролировать каждый элемент ограждающих конструкций, например, отдельную бетонную плиту стены. Размещать *акселерометр* можно только на поверхности основной несущей конструкции – кирпича, бетона, но не на штукатурке, побелке, обоях и т.п., так как последнее может привести к неверным результатам измерений.

Уровень тест-сигнала устанавливается в зависимости от решаемой задачи, но он обязательно должен превышать *шумы* в помещении не менее чем на 10 дБ. Обычно для измерения на окнах с одиночным стеклом достаточно звукового давления 60...65 дБ, для стеклопакетов – 70...80 дБ. При оценке дверных проемов, даже двойных без применения специальных средств звукоизоляции, – до 90 дБ.

Уровень тестовых акустических сигналов устанавливается (подбирается) таким образом, чтобы на всех средних частотах октавных полос обеспечивалась бы четкая фиксация контрольного (тестового) сигнала соответствующим измерительным датчиком.

При проведении измерений выбранный уровень этого тестового сигнала поддерживается постоянным.

Необходимо сказать о существующих автоматизированных комплексах для оценки защищенности акустической информации от утечки по акустическим и виброакустическим каналам. В качестве примера рассмотрим комплекс "Шепот", внешний вид которого представлен на рисунке.



Система оценки защищенности по виброакустическому и акустическому каналам «Шепот»

Система «Шепот» обеспечивает:

- автоматические измерения уровня звукового давления тестового сигнала вблизи и на удалении от его источника в 5-октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц;
- автоматические измерения уровня звукового давления тестового сигнала вблизи от его источника и уровня наведенного им виброускорения в 5-октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц;
- возможность перехода на ручное управление аппаратурой системы;
- использование данных измерений по 5-октавным полосам для расчета показателей защищенности и настройки системы защиты выделенных помещений по виброакустическому каналу утечки речевой информации;
- формирование и ведение базы данных о результатах выполненных измерений, включающей информацию о месте проведения измерений (объект, помещение, контрольная точка) и о результатах измерений и расчетов в каждой контрольной точке;
- составление отчета по результатам измерений в форме, отвечающей требованиям НМД АРР;
- автоматический и/или ручной режим ввода данных для расчета показателей защищенности выделенных помещений по виброакустическому каналу;
- установку параметров проведения измерений для каждого измерительного цикла;

- ввод калибровочных значений измерительных микрофонов и акселерометра, их сохранение и корректировку;
- расчет показателей защищенности помещений от утечки информации по акустическому и вибрационному каналам при заданных нормируемых показателях защищенности информации – отношениях «сигнал/шум» («сигнал/(помеха + шум)»);
- автоматические измерения уровня звукового давления тестового сигнала вблизи и на удалении от его источника в 19 третьоктавных полосах с центральными частотами 125, 160, 200, 250, 315, 400, 500, 630, 800, 1000, 1250, 1600, 2000, 2500, 3150, 4000, 5000, 6300 и 8000 Гц;
- автоматические измерения уровня звукового давления тестового сигнала вблизи от его источника и уровня наведенного им виброускорения в 19 третьоктавных полосах с центральными частотами 125, 160, 200, 250, 315, 400, 500, 630, 800, 1000, 1250, 1600, 2000, 2500, 3150, 4000, 5000, 6300 и 8000 Гц;
- расчет показателей защищенности выделенных помещений от утечки информации по оптикоэлектронному каналу;
- автоматический и/или ручной режим ввода данных для расчета показателей защищенности выделенных помещений от утечки информации по оптикоэлектронному каналу;
- настройку конфигурации системы применительно к марке используемого в ней измерительного оборудования;
- формирование акустических сигналов различных видов при использовании звуковой карты ПЭВМ в качестве генератора шумового сигнала.

Оформление результатов контроля включает:

- анализ полученных результатов;
- принятие по результатам контроля решения о выполнении норм защищенности речевой информации относительно каждого опасного средства речевой разведки;
- документальное оформление проведенного контроля (составление протокола контроля).

*Анализ* полученных результатов предусматривает *определение* достоверности проведенных измерений, выявление внешних факторов, оказывающих существенное влияние на результаты измерений.

Документальное оформление результатов контроля осуществляется путем составления протокола контроля с необходимыми таблицами. Результаты инструментального контроля должны быть оформлены по правилу протоколом, а также рекомендациями и предложениями по обеспечению выполнения норм противодействия акустической речевой разведке.

Проверка защищенности информации от НСД заключается в проверке соответствия эффективности мероприятий по защите информации установленным требованиям или нормам по безопасности информации. Тестируются все группы средств защиты от НСД, рассмотренные нами в предыдущих лекциях.

**Проверяется соответствие** описания технологического процесса обработки и хранения защищаемой информации реальному процессу.

**Оценивается возможность** переноса информации большего уровня конфиденциальности на информационный носитель меньшего уровня.

**Проводится анализ** разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретным ОТСС и штатному персоналу.

**Оценивается соответствие** разрешенных и запрещенных связей разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки.

Проверка, как правило, осуществляется с использованием программных и программно-аппаратных средств контроля защищенности. В качестве примера рассмотрим продукты одной фирмы-ООО «Центр безопасности информации».

Средство контроля защищенности от НСД «Ревизор 2 ХР» предназначено для контроля полномочий доступа к информационным ресурсам.

Реализуемые функции:

- отображение всей информации, содержащейся в ПРД (возможен только просмотр);
- сравнение структуры ресурсов АРМ, описанной в ПРД, с реальной структурой ресурсов;
- создание отчета по результатам сравнения;
- построение плана тестирования объектов АРМ;
- проверка реальных прав доступа пользователей к объектам доступа;
- создание отчета по результатам тестирования.

Сетевой сканер «Ревизор сети» версия 3.0 предназначен для обнаружения уязвимостей установленного сетевого программного и аппаратного обеспечения, использующего протоколы стека *TCP/IP*. Система имеет широкие возможности, одной из которых является *поиск* уязвимостей, содержащихся в базе данных угроз и уязвимостей ФСТЭК, рассмотренных нами ранее. Кроме того *программа* проводит *поиск* уязвимостей, содержащихся в *cve.mitre.org*, *ovaldb.altx-soft.ru*, *microsoft.com* и некоторых других источниках.

Средство фиксации и контроля исходного состояния программного комплекса «ФИКС» предназначено для контроля подсистемы обеспечения целостности. Основные возможности программы:

- фиксация исходного состояния программного комплекса;
- контроль исходного состояния программного комплекса;
- фиксация и контроль каталогов;
- контроль различий в заданных файлах (каталогах);
- возможность работы с длинными именами файлов и именами, содержащими символы кириллицы.

*Программа* поиска и гарантированного уничтожения информации на дисках «TERRIER» позволяет осуществить *контроль* уничтожения информации. Для проверки необходимо создать на конфиденциальном логическом диске *файл* с контрольной комбинацией символов, определить местонахождение секторов с помощью «TERRIER», удалить *файл* с помощью штатных средств и проконтролировать его удаление с помощью TERRIER.

## **Документирование результатов контроля. Требования к средствам контроля защищенности информации**

Следует отметить, что к средствам контроля эффективности мер защиты информации, как и к производителям таких средств, предъявляются достаточно жесткие требования. В соответствии с «Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации», утвержденным Постановлением Правительства 3 марта 2012 № 171, разработка и производство технических средств контроля эффективности мер защиты информации подлежит лицензированию. А сами разрабатываемые и производимые средства контроля эффективности мер защиты должны иметь *сертификат соответствия* ФСТЭК по требованиям Постановления Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

*Контроль* эффективности защиты завершается оформлением Заключения с краткой оценкой соответствия объекта информатизации по безопасности информации, конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями, совершенствованию этой системы, рекомендациями по контролю функционирования объекта информатизации. К Заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении *вывод*.

---

<sup>i</sup> <http://www.findpatent.ru/patent/220/2207618.html>

© FindPatent.ru – патентный поиск, 2012-2018