

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФБГОУ ВПО «Кубанский государственный аграрный университет»

Факультет прикладной информатики
Кафедра компьютерных технологий и систем

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Справочник по программно-аппаратным средствам защиты информации
(для бакалавров специальности «Бизнес-информатика»)

Краснодар
2013

УДК 004
ББК 32.81 я 7
И72

Рецензенты:

- доктор технических наук, профессор Атрощенко В.А. – декан факультета компьютерных технологий и автоматизированных систем ФГОУ ВПО "Кубанский государственный технологический университет";
- доктор экономических наук, профессор Луценко Е.В. – профессор кафедры компьютерных технологий и систем ФГБОУ ВПО "Кубанский государственный аграрный университет".

Лаптев В.Н.

Информационная безопасность: Справочник по программно-аппаратным средствам защиты информации (для бакалавров специальности « Бизнес-информатика»). / В.Н. Лаптев, С.В. Лаптев – Краснодар: КубГАУ, 2013. - 105 с.

В справочнике по представлены основные термины и определения, используемые в дисциплинах «Информационная безопасность». Он подготовлен для облегчения усвоения бакалаврами ФПИ КубГАУ теоретических и прикладных аспектов этой дисциплины в соответствии с требованиями ФГОС ВПО по специальности « Бизнес-информатика».

Он является обязательным приложением к курсу лекций и практикуму по дисциплине, так как обеспечивает качественное проведение лабораторных занятий и выполнение самостоятельной работы обучающимися по учебному курсу.

Рассмотрены и рекомендованы к изданию на заседании кафедры компьютерных технологий и систем КубГАУ __ сентября 2013 г., протокол №1.

Рекомендованы к печати:

- Советом факультета прикладной информатики Кубанского государственного аграрного университета __ сентября 2013 г., протокол № __.

© Лаптев Владимир Николаевич, Лаптев Сергей Владимирович

© Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Кубанский государственный аграрный университет", 2013.

Оглавление

1. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ШИФРОВАНИЯ	4
1.1 Основные термины и классификация средств криптографической защиты информации....	4
1.2 Требования к средствам криптографической защиты информации	6
1.3 Программные СКЗИ. Особенности и примеры.....	7
1.4 Аппаратные и аппаратно-программные СКЗИ. Особенности и примеры	9
1.5 Проблема выбора	10
1.6 Основные принципы построения СКЗИ	10
1.7 Принципы построения аппаратных СКЗИ	11
1.8 Принципы построения программных и программно-аппаратных СКЗИ.....	13
1.8.1 Методы разработки программных и программно-аппаратных СКЗИ.....	13
1.8.2 Обеспечение надежности программных и программно-аппаратных СКЗИ	14
1.8.3 Основные подходы к обеспечению качества СКЗИ	14
1.8.4 Обеспечение отказоустойчивости СКЗИ.....	14
2.8.5 Предотвращение неисправностей СКЗИ	15
2.8.6 Фаза анализа и спецификации требований.....	15
2.8.7 Фаза проектирования	16
2.8.8 Фаза исполнения	16
2.9 Специфические вопросы разработки программных СКЗИ	16
7.2. ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ ЗАЩИТЫ ОТ УДАЛЕННЫХ АТАК В СЕТИ INTERNET	70
7.2.1. Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети	71
1. Многоуровневая фильтрация сетевого трафика.	71
2. Проху-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте.....	71
3. Создание частных сетей (Private Virtual Network - PVN) с "виртуальными" IP-адресами (NAT - Network Address Translation).	71
7.2.2. Программные методы защиты, применяемые в сети Internet.....	73
7.2.2.1. SKIP-технология и криптопротоколы SSL, S-HTTP как основное средство	73
защиты соединения и передаваемых данных в сети Internet	73
7.2.2.2. Сетевой монитор безопасности IP Alert-1	74
Информация для клиентов	100
Авторизация	102
подготовка необходимой документации и проведение оценки соответствия информационной системы персональным данным требованиям безопасности информации (аттестация информационной системы персональным данным).	104
ЛИТЕРАТУРА И ИНТЕРНЕТ ИСТОЧНИКИ	104

1. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ШИФРОВАНИЯ

1.1 Основные термины и классификация средств криптографической защиты информации

К средствам криптографической защиты информации (СКЗИ), относятся

- аппаратные,
- программно-аппаратные и
- программные

средства, реализующие криптографические алгоритмы преобразования информации.

Предполагается, что СКЗИ используются в некоторой компьютерной системе (в ряде источников - информационно-телекоммуникационной системе или сети связи), совместно с механизмами реализации и гарантирования некоторой политики безопасности.

Наряду с термином "средство криптографической защиты информации" часто используется термин **шифратор** - аппарат или программа, реализующая алгоритм шифрования. Введенное понятие СКЗИ включает в себя шифратор, но в целом является более широким.

Первые операционные системы (ОС) для персональных компьютеров (MS-DOS и Windows версий до 3.1 включительно) вовсе не имели собственных средств защиты, что и породило проблему создания дополнительных средств защиты. Актуальность этой проблемы практически не уменьшилась с появлением более мощных ОС с развитыми подсистемами защиты. Это обусловлено тем, что большинство систем не способны защитить данные, находящиеся за ее пределами, например, при использовании сетевого информационного обмена.

Средства криптографической защиты информации, обеспечивающие повышенный уровень защиты можно разбить на пять основных групп (рисунок 1.1).

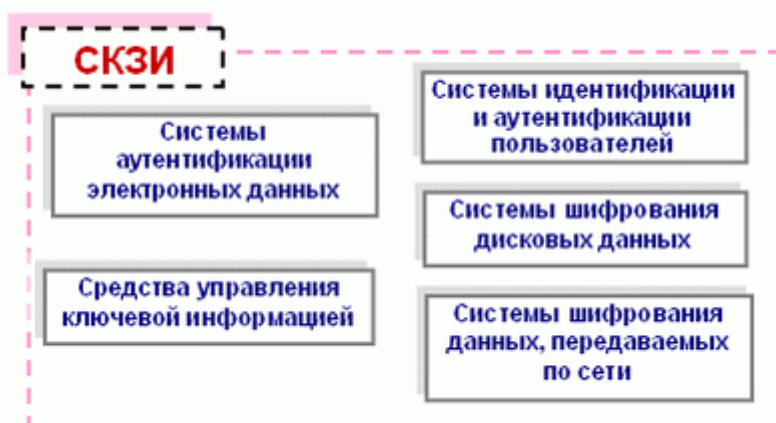


Рисунок 1.1 Основные группы СКЗИ

Первую группу образуют системы идентификации и аутентификации пользователей. Такие системы применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы этих систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Вторую группу средств, обеспечивающих повышенный уровень защиты, составляют системы шифрования дисковых данных. Основная задача, решаемая такими системами, состоит в защите от несанкционированного использования данных, расположенных на дисковых носителях.

Обеспечение конфиденциальности данных, располагаемых на дисковых носителях, обычно осуществляется путем их шифрования с использованием симметричных алгоритмов шифро-

вания. Основным классификационным признаком для комплексов шифрования служит уровень их встраивания в компьютерную систему.

Системы шифрования данных могут осуществлять криптографические преобразования данных:

- на уровне файлов (защищаются отдельные файлы);
- на уровне дисков (защищаются диски целиком).

К программам первого типа можно отнести архиваторы типа WinRAR, которые позволяют использовать криптографические методы для защиты архивных файлов.

Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities.

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования.

По способу функционирования системы шифрования дисковых данных делят на два класса:

- системы “прозрачного” шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах *прозрачного шифрования* (шифрования “на лету”) криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Ярким примером является шифрование папки Temp и Мои документы при использовании EFS Win2000 – при работе шифруются не только сами документы, но и создаваемые временные файлы, притом пользователь не замечает этого процесса.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

К третьей группе средств, обеспечивающих повышенный уровень защиты, относятся системы шифрования данных, передаваемых по компьютерным сетям. Различают два основных способа шифрования:

- канальное шифрование;
- оконечное (абонентское) шифрование.

В случае *канального шифрования* защищается вся передаваемая по каналу связи информация, включая служебную. Соответствующие процедуры шифрования реализуются с помощью протокола канального уровня семиуровневой эталонной модели взаимодействия открытых систем OSI (Open System Interconnection).

Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Однако, у данного подхода имеются существенные недостатки, в частности, шифрование служебной информации, неизбежное на данном уровне, может привести к появлению статистических закономерностей в зашифрованных данных; это влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя прикладными объектами (абонентами). Оконечное шифрование реализуется с помощью протокола прикладного или представительного уровня эталонной модели OSI. В этом случае защищенным оказывается только содержание сообщения, вся служебная информация остается открытой. Данный способ позволяет избежать проблем, связанных с шифрованием служебной информации, но при этом возникают другие проблемы. В частности, злоумышленник, имеющий доступ к каналам связи компьютерной сети, получает возможность анализировать информацию о структуре обмена сообщениями, например, об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

Четвертую группу средств защиты составляют системы аутентификации электронных данных.

При обмене электронными данными по сетям связи возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе.

Для аутентификации электронных данных применяют код аутентификации сообщения (имитовставку) или электронную цифровую подпись. При формировании кода аутентификации сообщения и электронной цифровой подписи используются разные типы систем шифрования.

Пятую группу средств, обеспечивающих повышенный уровень защиты, образуют средства управления ключевой информацией. Под ключевой информацией понимается совокупность всех используемых в компьютерной системе или сети криптографических ключей.

Как известно, безопасность любого криптографического алгоритма определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в компьютерной системе или сети.

Основным классификационным признаком средств управления ключевой информацией является вид функции управления ключами. Различают следующие основные виды функций управления ключами: генерация ключей, хранение ключей и распределение ключей.

Способы *генерации ключей* различаются для симметричных и асимметричных криптосистем. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем представляет существенно более сложную задачу в связи с необходимостью получения ключей с определенными математическими свойствами.

Функция *хранения ключей* предполагает организацию безопасного хранения, учета и удаления ключей. Для обеспечения безопасного хранения и передачи ключей применяют их шифрование с помощью других ключей. Такой подход приводит к *концепции иерархии ключей*. В иерархию ключей обычно входят главный ключ (мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключей являются критическими вопросами криптографической защиты.

Распределение ключей является самым ответственным процессом в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также оперативность и точность их распределения. Различают два основных способа распределения ключей между пользователями компьютерной сети:

- применение одного или нескольких центров распределения ключей;
- прямой обмен сеансовыми ключами между пользователями.

Перейдем к формулированию требований к СКЗИ, общим для всех рассмотренных классов.

1.2 Требования к средствам криптографической защиты информации

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

1. зашифрованное сообщение должно поддаваться чтению только при наличии ключа, попытка же чтения без предварительного знания ключа должна быть необходимо сопряжена с вычислительно сложной задачей, время решения которой на современной компьютерной технике превышает время жизни защищаемой информации;

2. 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. Вообще говоря, в среднем при лобовой атаке криптоаналитику приходится перебрать половину всех возможных ключей, но в наихудшем случае ему придется перебрать все ключи;

3. 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 распределенных вычислений);

4. знание алгоритма шифрования не должно влиять на надежность защиты (принцип Кирхгофа);
5. незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения – так называемый принцип распространения ошибки;
6. структурные элементы алгоритма шифрования должны быть неизменными, т.е. должен быть реализован их контроль целостности;
7. дополнительные биты, вводимые в сообщение в процессе шифрования, (например, при дополнении открытого текста до длины, кратной длине блока алгоритма шифрования) должны быть полностью и надежно скрыты в шифрованном тексте;
8. длина шифрованного текста должна быть равной длине открытого текста;
9. не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
10. любой ключ из множества возможных должен обеспечивать надежную защиту информации, т.е. из ключевого множества должны быть исключены заведомо слабые ключи. К таким могут относиться не только ключи, не удовлетворяющие требованиям статистической независимости и равновероятности знаков, но и некоторые специфические для данного алгоритма шифрования;
11. алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

1.3 Программные СКЗИ. Особенности и примеры

Как уже указывалось, основным достоинством программных СКЗИ является их дешевизна и гибкость. Наряду с этими существенными достоинствами у программных СКЗИ имеются и существенные недостатки, заключенные, собственно, в их наибольшем достоинстве – возможности легкой модификации. Программа, реализующая некоторую функцию защиты информации, может быть достаточно просто модифицирована злоумышленником. Для устранения угрозы модификации следует каким-то образом осуществить контроль целостности этой программы, однако это возможно только с помощью другой программы. Проверка целостности одних программ при помощи других не является надежной. Необходимо четко представлять, каким образом обеспечивается целостность собственно программы проверки целостности. Если обе программы находятся на одних и тех же носителях, доверять результатам такой проверки нельзя.

Еще одной серьезной проблемой программных СКЗИ является использование оперативной памяти системы для операций с криптографическим ключом – конечный промежуток времени криптографический ключ присутствует в памяти в открытом виде и может быть из нее извлечен. Кроме того, есть еще одна проблема, связанная скорее с недостатками программирования, а не со спецификой программных СКЗИ, например, неаккуратное использование временных файлов, при котором в них может оставаться ценная для криптоанализа информация.

Весьма серьезной проблемой программных СКЗИ является датчик случайных чисел, используемых для формирования ключа. Часто для генерации ключевого материала используются показания системных часов, данные из оперативной памяти, и прочая псевдослучайная информация. Следует отметить, что ни один метод получения случайного числа, кроме физически случайных (например, тепловой шум) не может быть признан истинно случайным и, вполне вероятно, подчиняется некоторой закономерности, а, следовательно, при его использовании может быть получен слабый ключ. В некоторых современных компьютерах имеется встроенный аппаратный датчик случайных чисел, однако в контексте использования программных СКЗИ

следует помнить, что этот датчик доступен ОС, поэтому для его гарантированной стойкости необходимо использование доверенной ОС.

В связи с перечисленным к программным системам защиты информации следует относиться с особой осторожностью, хотя они могут быть весьма эффективны для защиты информации, не содержащей государственной тайны (таблица 2.1).

Таблица 1.1. – Примеры систем СКЗИ

Группа СКЗИ	Примеры
Системы идентификации и аутентификации пользователей	Встроенные средства ОС
Системы шифрования дисковых данных	Встроенные средства ОС, PGP, Secret Disk
Системы шифрования данных, передаваемых по сетям	Комплексы ЗАСТАВА (VPN + программное СКЗИ)
Системы аутентификации электронных данных	PGP
Средства управления ключевой информацией	Сервер сертификатов ЗАСТАВА

В большинстве распространенных операционных систем предусмотрены встроенные средства шифрования дисковых данных. Например, в MS Windows, начиная с Windows 2000, предусмотрена система шифрования файлов на NTFS -дисках. Это прозрачное шифрование, технология которого основана на сертификатах открытых ключей.

Такие криптографические сервисы, как контроль целостности, аутентификацию пользователей и данных, шифрование дисковых данных и канальное шифрование можно реализовать, используя базовые криптографические примитивы: хеш-функции, схемы шифрования и электронно-цифровой подписи. Это делает обоснованным иерархический подход к созданию СКЗИ: на базе основного устройства (аппаратного или программного), реализующего основные криптографические примитивы. Посредством использования библиотек функций создаются прикладные программные продукты, осуществляющие дисковое (в т.ч. прозрачное), абонентское, канальное шифрование, ЭЦП, аутентификацию пользователей и данных. Такой подход реализован, например, в разработках фирмы "Анкад", где основным устройством являются платы КРИПТОН или программный эмулятор платы Crypton Emulator (рисунок 1.2).

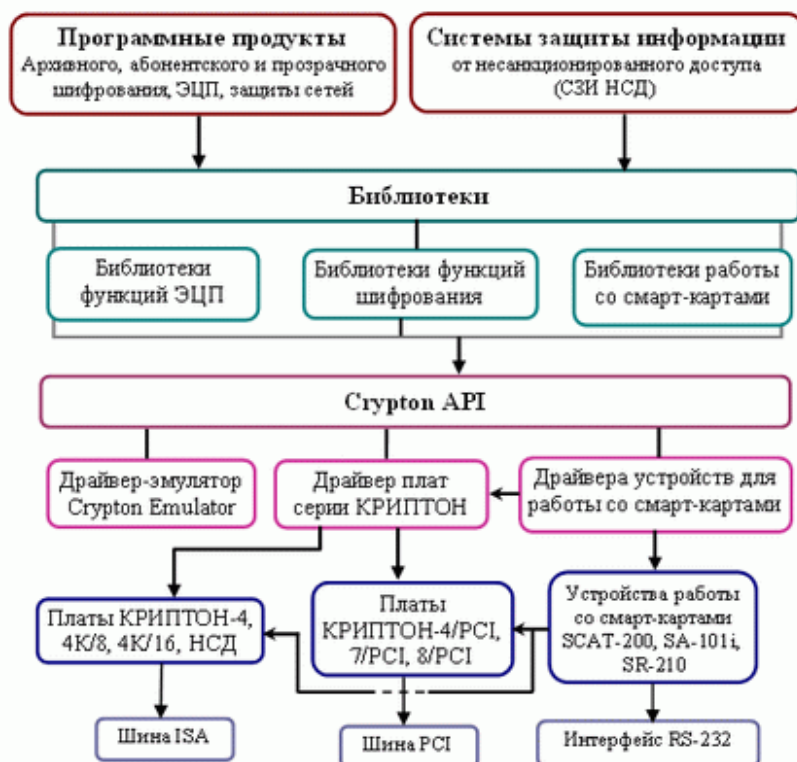


Рисунок 1.2 Структура средств криптографической защиты информации фирмы "Анкад"

Во многом аналогичный подход использован Microsoft при создании своего CryptoAPI – криптографического интерфейса прикладных программ. CryptoAPI представляет собой набор функций, предназначенных для работы различных криптографических сервисов (шифрования, хэш-функций, ЭЦП, проверки сертификатов). С помощью функций CryptoAPI можно создавать прикладное ПО, призванное решать криптографические задачи различной степени сложности. Особо стоит отметить, что CryptoAPI содержит только описание функций криптографических примитивов; непосредственная их реализация содержится в отдельной библиотеке, называемой криптопровайдером. Microsoft предоставляет два своих криптопровайдера – простой и расширенный. Они содержат реализацию криптографических функций, используемых ОС Windows для собственных нужд.

Таким образом, CryptoAPI позволяет, с одной стороны, использовать криптографические средства Windows, а с другой, не ограничивает программиста своей собственной реализацией криптоалгоритмов, позволяя использовать другие (доверенные) криптопровайдеры. При этом следует учитывать, что используя криптопровайдер от Microsoft, мы выдаем определенный кредит доверия самой ОС Windows, несмотря на закрытость ее кода и фактическую невозможность установить факт отсутствия ошибок, программных закладок недобросовестных разработчиков или соответствующих служб. Кроме того, криптопровайдер от Microsoft содержит описание ограниченного количества алгоритмов шифрования и имеет ряд весьма неприятных для разработчика СКЗИ ограничений.

Следует отдельно отметить развивающееся семейство программных СКЗИ, созданных в рамках концепции open source. В первую очередь к ним следует отнести детище Филипа Циммермана – PGP. PGP – программное СКЗИ, позволяющее (в зависимости от версии функциональность может различаться) шифровать данные (файловое шифрование или создание защищенного диска – PGP-диск), подписывать сообщения и управлять ключами. Следует отметить, что в настоящее время проект PGP принадлежит Network Associates и Циммерман не имеет к нему более никакого отношения.

1.4 Аппаратные и аппаратно-программные СКЗИ. Особенности и примеры

В первую очередь к аппаратным СКЗИ для сохранения исторической справедливости следует отнести шифраторы докомпьютерной эры. Это табличка Энея, шифровальный диск Альберти, и, наконец, дисковые шифрующие машины. Самым видным представителем дисковых шифрмашин стал шифратор времен второй мировой войны Enigma. Современные СКЗИ нельзя строго отнести к аппаратным, их было бы правильнее называть аппаратно-программными, однако, поскольку их программная часть неподконтрольна ОС, в литературе их часто называют аппаратными. Основной особенностью аппаратных СКЗИ является аппаратная реализация (за счет создания и применения специализированных процессоров) основных криптографических функций – криптографических преобразований, управления ключами, криптографических протоколов и т. д.

Аппаратно-программные средства криптографической защиты информации сочетают гибкость программного решения с надежностью аппаратного. При этом за счет гибкой программной оболочки можно быстро менять пользовательский интерфейс, конечные функции продукта, производить его конечную настройку; а аппаратная компонента позволяет защитить от модификации алгоритм криптографического примитива, обеспечить высокую защищенность ключевого материала и зачастую более высокую скорость работы.

Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, для внесения изменений в ПО необходимо получить доступ к соответствующей плате и заменить микросхему. В случае использования универсального процессора реализация подобных действий потребует применения специального оборудования, что еще более затруднит проведение атаки. Использование специ-

ализированного процессора с реализацией алгоритма работы в виде интегральной микросхемы полностью снимает проблему нарушения целостности этого алгоритма.

На практике зачастую функции аутентификации пользователя, проверки целостности, криптографические функции, образующие ядро системы безопасности, реализуются аппаратно, все остальные функции – программно.

Приведем несколько примеров аппаратно-программных СКЗИ (таблица 1.2).

Таблица 1.2.- Примеры аппаратно-программных СКЗИ

Группа СКЗИ	Примеры
Системы идентификации и аутентификации пользователей	АККОРД
Системы шифрования дисковых данных	Crypton Soft, ГРЯДА
Системы шифрования данных, передаваемых по сетям	Crypton ArcMail (базовое устройство – плата КРИПТОН)
Системы аутентификации электронных данных	Crypton Sign, Crypton ArcMail (базовое устройство – плата КРИПТОН)
Средства управления ключевой информацией	Crypton Tools базовое устройство – плата КРИПТОН)

В приведенной таблице предпочтение отдано отечественным производителям, что не является определяющим фактором при выборе СКЗИ, если нет каких-либо дополнительных требований.

1.5 Проблема выбора

На сегодняшний день пользователи средств защиты информации, реализующих криптографические технологии, осуществляют свой выбор на основании ряда критериев, среди которых можно выделить:

- надежность криптоалгоритмов (длина ключа, стойкость алгоритма);
- легальность использования в соответствии с существующими стандартами и нормативно-правовой базой;
- наличие сертификатов государственных органов;
- экспортно-импортные ограничения.

Кроме собственно выбора алгоритма, не менее остро стоит проблема выбора способа реализации: аппаратная (аппаратно-программная) или чисто программная. Основным критерием здесь становится стоимость защищаемой информации и величина бюджета компании на цели приобретения и эксплуатации СКЗИ.

1.6 Основные принципы построения СКЗИ

С ростом сложности средств связи и информационных технологий возрастает и сложность обеспечения безопасности с помощью СКЗИ. Об этом говорят как западные исследования, проводимые с начала 80-х годов, так и отечественные работы настоящего времени. Основные трудности связаны со следующими факторами:

- средство реализации криптографического алгоритма в компьютерной системе представляет собой равноправный с прочими ресурс (является программой и использует данные компьютерной системы);
- ключевая информация СКЗИ является данными компьютерной системы с возможностью доступа со стороны других программ и с прохождением при обработке также через ряд внешних по отношению к СКЗИ программных модулей;
- функционирование СКЗИ происходит не автономно, а выполняется под управлением операционной системы и различных программ-посредников, которые, при желании, могут произвольно искажать вводимую и выводимую СКЗИ информацию;
- программная среда, в которой работает СКЗИ, устроена иерархично, т.е. для выполнения типовых функций все программы используют одни и те же фрагменты кода и данные;

- работа СКЗИ сопряжена с возникновением ошибочных ситуаций в аппаратной и программной среде компьютерной системы.

В связи с этим для обеспечения безопасности информации в современных информационно-телекоммуникационных системах, основанных на передовых информационных технологиях, необходимо эффективно решать следующий круг сложных научно-технических задач:

- обеспечивать оптимальную, формально проверяемую реализацию криптографических алгоритмов в рамках эксплуатируемых в информационно-телекоммуникационных системах программных и аппаратных платформ;
- обеспечивать при проектировании СКЗИ меры обеспечения отказоустойчивости, защиты от сбоев и искажений аппаратной компоненты;
- обеспечивать защищенность СКЗИ и его ресурсов (ключевой информации и др.) от несанкционированного доступа со стороны других программ;
- гарантировать качество управления СКЗИ со стороны операционной системы и программ-посредников, в том числе и в условиях ошибочных и преднамеренных действий пользователей.

Следует также отметить, что реализация СКЗИ в сложных универсальных операционных средах типа Windows или Unix требует проведения значительных объемов поисковых исследований для определения точек встраивания СКЗИ в операционную систему и обеспечения корректности их работы.

Разработка всякого технического средства начинается с формулирования технического задания. Специфика криптографических средств защиты информации определяет следующие обязательные разделы ТЗ:

1. точное назначение данных СКЗИ;
2. реализуемые СКЗИ функции;
3. требования по уровню защиты информации;
4. требования по производительности криптографических преобразований;
5. требования по защите от НСД (инженерной криптографии);
6. реальные условия эксплуатации;
7. специальные требования;
8. требования к программному обеспечению.

Важнейшим этапом построения СКЗИ является тестирование.

Перейдем к описанию принципов построения СКЗИ.

1.7 Принципы построения аппаратных СКЗИ

Концепция построения аппаратных СКЗИ ставит две основных цели:

- максимальное повышение уровня защиты информации и защиты от НСД;
- максимальное увеличение быстродействия криптопреобразований.

Для повышения уровня защиты информации и защиты от НСД могут быть использованы следующие методы инженерной криптографии:

1. обеспечение минимально возможного взаимодействия прикладного ПО и ОС персонального компьютера (ПК) с аппаратными средствами (АС) за счёт:
 - использования специального командного (процедурного) интерфейса взаимодействия прикладного ПО с АС, обеспечивающего невозможность прямого доступа прикладного ПО и ОС к ресурсам АС (памяти, процессору и т. п.) и предусматривающего обязательную первоначальную инициализацию АС с применением ключей (паролей) доступа заданной длины (не менее 8 байт);
 - взаимодействия прикладного ПО (ОС) с АС через "прозрачный" для пользователя "почтовый ящик" (буфера обмена: приёмный и передающий, физически расположенные в АС и недоступные для прямого чтения/записи прикладному ПО и ОС);
 - хранения криптографических алгоритмов (исполняемых модулей) в энергонезависимой памяти (ЭНП) АС в зашифрованном виде (т. о. отпадает необходимость загрузки алгоритмов "извне").

2. применение резервированного (дублированного) генератора случайных чисел для формирования физических ключей заданной длины;
3. загрузка исполняемых криптографических алгоритмов из энергонезависимой памяти во встроенное ОЗУ (RAM) микропроцессора в шифрованном виде;
4. исполнение криптографических алгоритмов только из встроенного ОЗУ микропроцессора (с предварительным расшифрованием непосредственно в данном ОЗУ);
5. хранение шифрованных данных в ЭНП в структурированном виде с применением различных методов контроля (например, контрольное суммирование загружаемых программных модулей) для обеспечения контроля достоверности и целостности информации;
6. передача данных (ключевой информации, загружаемых криптографических алгоритмов, результатов промежуточных вычислений и т. д.) по внутренним шинам АС только в шифрованном виде;
7. "прошивка" отдельных ключей (например, ключа, который используется при инициализации АС) в "железе" с обеспечением гарантированной невозможности извлечения;
8. применение "оперативно загружаемой схемотехники" в аппаратных ускорителях;
9. использование внешних ключей, загружаемых пользователем по отдельному интерфейсу со специальных внешних накопителей (электронная карточка ридера, например);
10. применение в АС специального защитного экрана, обеспечивающего защиту от НСД самого АС (при необходимости);
11. включение в состав АС аппаратного расширения BIOS ПК, позволяющего контролировать (до загрузки ОС) целостность ОС и прикладного ПО (например, физически расположенного на жестком диске ПК).

Важным требованием является возможность полного самотестирования АСКЗИ, выполняемого каждый раз после аппаратного (по включению питания) или программного сброса. Алгоритмы самотестирования должны быть встроенными в АСКЗИ.

Повышение производительности криптографических операций может осуществляться за счёт:

- применения в качестве ядра АСКЗИ максимально адаптированных для реализации большинства криптографических алгоритмов\операций современных высокопроизводительных микропроцессоров (сигнальных процессоров DSP) на основе RISC архитектуры;
- применения "оперативно загружаемой схемотехники" аппаратных ускорителей (необходимых в ряде случаев), которые на аппаратном уровне реализуют отдельные элементы криптографических алгоритмов (например, таблицу подстановок в ГОСТ-28147) или полностью криптографические алгоритмы (например, DES) и которые не совсем оптимально "ложатся" на ядро АСКЗИ (микропроцессор) с точки зрения временных затрат на их исполнение;
- применения в отдельных обоснованных случаях многопроцессорных структур.

Следует отметить, что современные АСКЗИ могут быть адаптированы к требованиям конечного пользователя за счёт перепрограммирования и/или расширения системного ПО (BIOS), встроенного в АСКЗИ.

Специальные требования накладывают ограничения на конструктивное исполнение АСКЗИ (топологию печатной платы и т. д.) в части:

1. допустимого уровня электромагнитных помех, излучаемых АСКЗИ;
2. помехозащищённости АСКЗИ;
3. защиты от электростатического разряда;
4. защиты от внешних электромагнитных полей;
5. защиты от электрических перегрузок;
6. защиты от тепловых перегрузок (перегрева).

Эти требования должны быть сформулированы в техническом задании на АСКЗИ, а их выполнение проконтролировано при приеме в эксплуатацию.

Повышение надёжности АСКЗИ может быть достигнуто за счёт "горячего" резервирования (дублирования/троирования) АСКЗИ. Практическая целесообразность такого резервирования

ния определяется свойствами защищаемой информации. Возможны два варианта реализации резервирования:

- установка 2/3 одноканальных плат АСКЗИ в соответствующие свободные слоты шины ISA/PCI/ USB персонального компьютера;
- разработка специального конструктивного решения АСКЗИ со встроенными двумя-тремя каналами резервирования.

Недостатком в обоих случаях является, как правило, не резервированный ПК, в который устанавливается АСКЗИ.

1.8 Принципы построения программных и программно-аппаратных СКЗИ

1.8.1 Методы разработки программных и программно-аппаратных СКЗИ

В соответствии с принципом абстракции при проектировании СКЗИ разработчики могут идти по меньшей мере двумя путями: от аппаратуры "вверх" – к программному обеспечению, реализующему пользовательский интерфейс, или, наоборот, от заданного набора пользовательских функций "вниз" – к реальному оборудованию.

Это и есть два основных метода проектирования – метод снизу вверх и метод сверху вниз. Остальные описываемые методы по своей сути сводятся к этим двум или являются их сочетанием.

Метод "снизу вверх" предполагает проектирование начинается с основного аппаратного оборудования системы. При проектировании все модули системы разбиваются на ряд слоев, причем нулевой слой образует аппаратура. Каждый следующий слой последовательно добавляет новые функции, используя уже реализованные в предыдущих слоях. На самом верхнем слое должна достигаться функциональность, полностью отвечающая всем требованиям, поставленным перед разработчиком.

К недостаткам метода проектирования снизу вверх относят:

- необходимость с самого начала принимать решение о выборе способа реализации компонент СКЗИ – с помощью аппаратуры, микропрограмм или программ, что сделать очень трудно;
- возможность проектирования программной части только после разработки аппаратуры;
- расхождение между конечным продуктом и определенным в техническом задании (ТЗ).

При разработке программ, реализующих криптографические алгоритмы, данный метод применим только отчасти и только в тех случаях, если система команд процессора, на котором будет работать проектируемая программа, имеет в своем составе специфичные команды, реализующие элементарные базовые криптографические преобразования, либо если предполагается использовать уже готовое аппаратное обеспечение (разработанное ранее, приобретенное готовое или, быть может, регламентированное требованиями ТЗ).

При использовании *метода проектирования "сверху вниз" (иерархический метод)* исходят от того набора пользовательских функций, которые должны быть реализованы в разрабатываемой системе и последовательно, выделяя отдельные слои, опускаются вплоть до аппаратуры. В этом случае процесс проектирования заключается в следующей последовательности.

Определяется абстракция описания компонент СКЗИ высшего уровня. Далее систематически проводится анализ, достаточно ли определены компоненты, чтобы можно их было реализовать, используя некоторые примитивные понятия. Если нет, то каждая функция каждой компоненты представляется функциями компонент следующего слоя, которому соответствует более низкий уровень абстракции, и снова проводится анализ на возможность их реализации.

В иерархическом методе целесообразно использовать принцип модульного проектирования и структурный принцип.

Принцип модульного проектирования заключается в разделении программ на функционально самостоятельные части (модули), обеспечивающие заменяемость, кодификацию, удаление и дополнение составных частей.

Преимущества использования модульного принципа состоят в следующем:

- упрощается отладка программ, т.к.. ограниченный доступ к модулю и однозначность его внешнего проявления исключает влияние ошибок в других, связанных с ним, модулях на его функционирование;

- обеспечивается возможность организации совместной работы коллективов разработчиков, т. к. каждый программист имеет дело с независимой от других частью программы;

- повышается качество программы, т.к. относительно малый размер модулей и, как следствие, небольшая сложность их, позволяют провести более полную проверку программы.

Структурный принцип имеет фундаментальное значение и составляет основу большинства реализаций. Согласно этому принципу, для построения программы требуются только три основных составляющих блока:

- функциональный блок;
- конструкция обобщенного цикла;
- конструкция принятия двоичного решения.

Структурный принцип формализует процесс проектирования, позволяя постепенно продвигаться от более абстрактных функциональных блоков к более конкретным, до тех пор, пока каждый из них может быть реализован с помощью имеющихся функций либо языка программирования, либо операционной системы, либо с помощью аппаратных средств.

1.8.2 Обеспечение надежности программных и программно-аппаратных СКЗИ

В современных условиях, при создании средств криптографической защиты информации одним из ключевых моментов программной или программно-аппаратной реализации алгоритма является обеспечение его качества или, как еще принято говорить, надежности.

В общем случае под надежностью понимается свойство объекта сохранять во времени значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортировки.

Несмотря на определенный универсализм приведенного определения, между надежностью аппаратных средств и программного обеспечения имеется принципиальное различие. Программа в большинстве случаев не может отказать случайно. Ошибки в программном обеспечении, допущенные при его создании, зависят от технологии, от организации и квалификации исполнителей и, в принципе, не являются функцией времени.

Имеющийся опыт разработки программных шифраторов показывает, что любые, даже самые незначительные на первый взгляд, ошибки приводят к нежелательным последствиям. Поэтому, для современных программных систем обязательным требованием становится не просто реализация технического задания, или, в частном случае, алгоритма, а его реализация с надлежащим качеством.

1.8.3 Основные подходы к обеспечению качества СКЗИ

Существуют два основных общепринятых подхода к обеспечению качества СКЗИ от угрозы отказа функционирования, которые применимы, в том числе, и к программам, реализующим криптографические алгоритмы. Это отказоустойчивость (fault tolerance) и предотвращение неисправностей (fault avoidance).

Отказоустойчивость предусматривает, что ошибки, которые не удалось выявить на этапе разработки и тестирования СКЗИ, обнаруживаются во время работы программы и парируются за счет использования программной, информационной и временной избыточности. Предотвращение неисправностей связано с анализом природы ошибок, возникающих на разных фазах этапа разработки СКЗИ, и причин их возникновения.

1.8.4 Обеспечение отказоустойчивости СКЗИ

Из-за невозможности обеспечения абсолютной надежности программных и программно-аппаратных СКЗИ при разработке, даже при отсутствии злоумышленных воздействий, разработчики используют методы оперативного обнаружения дефектов при выполнении программ и искажений данных путем введения в них временной, информационной и программной избыточности. Эти же виды избыточности используются для оперативного восстановления искаженных данных.

Временная избыточность состоит в использовании некоторой части производительности ЭВМ для контроля исполнения программ и восстановления (рестарта) вычислительного процесса.

Так, например, в состав СКЗИ может быть введена процедура периодического контроля. Для борьбы со сбоями возможно применить процедуры периодического контроля, которые сводятся к выполнению предопределенных детерминированных тестовых процедур (для функций шифрования это может быть, например, прогон тестовых примеров).

Информационная избыточность состоит в дублировании накопленных исходных и промежуточных данных, обрабатываемых программами. Избыточность используется для обеспечения достоверности данных при проведении криптографических преобразований и обычно реализуется в виде вычисления имитовставок.

Программная избыточность используется для контроля и обеспечения достоверности наиболее важных решений по управлению и обработке информации. Она заключается в сопоставлении результатов обработки одинаковых исходных данных разными программами и исключения искажения результатов, обусловленных различными аномалиями.

Вместе с тем, обеспечение отказоустойчивости программной реализации СКЗИ, хотя и направлено в целом на повышение надежности, не может решить такую проблему, как обеспечение соответствия программной реализации криптографическому алгоритму. Для решения этой проблемы используют методы предотвращения неисправностей.

2.8.5 Предотвращение неисправностей СКЗИ

Основные подходы к предотвращению неисправностей связаны с анализом природы возникновения ошибок, возникающих при разработке программных и программно-аппаратных СКЗИ, что в свою очередь подразумевает анализ самого процесса разработки.

Процесс разработки СКЗИ принято описывать моделями жизненного цикла программ различных классов и назначения. В модели жизненный цикл структурируется рядом крупных фаз или этапов, каждый из которых характеризуется достаточно определенными целями и результатами. Анализ существующих наработок в данной области позволяет сделать вывод о том, что основными фазами создания СКЗИ являются:

- анализ и спецификация требований;
- проектирование;
- исполнение.

Рассмотрим содержание каждой из фаз, в контексте решения задачи предотвращения неисправностей СКЗИ.

2.8.6 Фаза анализа и спецификации требований

Анализ всей совокупности требований к системе – технического задания – выполняется на начальной фазе создания программ. ТЗ составляется на основании перечня требований, предъявленных к системе заказчиком (классы решаемых задач, их характеристики и особенности, режим работы автоматизированной системы, сопряжение с внешними объектами, пропускная способность, время ответа и т.п. при заданных ограничениях на стоимость, длительность разработки и др.). Цель создания ТЗ – уточнить и сформулировать задачи, возлагаемые на систему, согласовать требования заказчика и возможности исполнителя, составить техническое задание на разработку СКЗИ. Это делается для того, чтобы удостовериться в том, что от программ требуются только те системные требования, которые могут быть достигнуты.

Достоинства формальных методов заключается в том, что системы, разработанные с использованием подобного подхода, имеют принципиально высокое качество. При этом повышение качества достигается двумя путями:

- построением спецификаций в виде ясного, исчерпывающего, недвусмысленного и легкого для проверки математического утверждения;
- осуществлением верификации во время разработки СКЗИ.

Разработка формальной спецификации требует значительных усилий. Однако, как показывает практика, большинство ошибок, обнаруживаемых в конце жизненного цикла программ, и, следовательно, наиболее дорогих и сложных для исправления, возникает из-за ошибок в специ-

фикации. Таким образом, для предотвращения неисправностей СКЗИ рассмотренной фазе создания необходимо уделять особенное внимание.

С фазой анализа и спецификацией требований связаны системные ошибки. *Системные ошибки* определяются прежде всего неполной информацией о реальных процессах, происходящих в источниках и потребителях информации. Применительно к реализации криптографических алгоритмов можно говорить о неверном понимании, либо трактовке элементов алгоритма.

2.8.7 Фаза проектирования

Фаза проектирования как самостоятельный этап в большей степени может быть выделена при проектировании сложных программных комплексов, составной частью которых являются модули криптографических преобразований. В случае реализации самих модулей криптографических преобразований, фаза проектирования может быть выражена не столь отчетливо, или практически отсутствовать.

С фазой проектирования связаны алгоритмические ошибки. К алгоритмическим относят ошибки, обусловленные некорректной постановкой задач, решаемых отдельными частями ПО. К ним также относят ошибки связей модулей и функциональных групп программ. В большинстве случаев их также можно свести к ошибкам в спецификациях.

2.8.8 Фаза исполнения

Фаза исполнения включает в себя кодирование, интегрирование, а также тестирование и отладку. С ней связаны программные ошибки. Программные ошибки по количеству и типам, в первую очередь, определяются степенью автоматизации программирования и глубиной формализованного контроля текстов программ. Программные ошибки сильно зависят от выбранного языка программирования. Имеющаяся статистика показывает, что наибольший вес имеют ошибки неполной программной реализации функций алгоритма или неверный порядок реализации функций.

Таким образом, на основании анализа фаз создания СКЗИ и допускаемых на них ошибок можно сделать вывод о том, что двумя основными разновидностями ошибок являются:

- неверное специфицирование как всего программного комплекса, так и отдельных его составляющих;
- функциональное несоответствие программы алгоритму.

Предотвращение данных ошибок – путь к обеспечению защиты от сбоев и неисправностей СКЗИ, а также обеспечение точной реализации заданных криптографических алгоритмов в программных и программно-аппаратных СКЗИ.

1.9 Специфические вопросы разработки программных СКЗИ

С точки зрения защиты информации программные средства с криптографическими функциями для универсальных ЭВМ являются гораздо более уязвимыми, нежели специализированные шифраторы. Это обусловлено тем, что при создании всевозможных текстовых редакторов, СУБД, коммуникационных программ, архиваторов и т.д. их разработчики в первую очередь руководствуются принципом максимального удобства для пользователя и принципом безотказного функционирования, а вопросы гарантированной защиты отодвигаются на второй и даже третий план. Принципы безотказного функционирования и удобства программных продуктов диктуют необходимость введения различных видов избыточности, в частности, таких понятий как формат носителя данных и формат файла. Как следствие использование форматов приводит к ослаблению криптографической схемы. С учетом того, что весьма часто алгоритмы криптографической защиты реализуются не специалистами-криптографами, а программистами, не имеющими специальной подготовки, можно отметить относительно невысокую стойкость большинства широко распространенных программных средств с криптографическими функциями.

Основными причинами низкой криптостойкости, как правило, являются следующие:

- применение нестойких криптоалгоритмов;
- слабость ключевой системы;
- ошибки в проектировании программ.

Наиболее опасными и трудноустраняемыми являются ошибки проектирования – зачастую подсистема криптографической защиты информации не задумывается изначально, а добавляет-

ся к уже существующему продукту, что не позволяет учесть все возможные проблемы применения криптографии. Например, встроенное средство шифрования документов Microsoft Word XP реализует стойкий криптоалгоритм и достаточно корректную ключевую систему, однако из-за того, что формат хранения документов предусматривает возможность хранения нескольких версий одного и того же документа в одном файле (зашифрованных одним ключом), криптоаналитик может восстановить ключ шифрования

<http://www.npp-bit.ru/katalog2/po/>

Сайт компании ЗАО "НПП "БИТ"

ЗАО «НПП «БИТ» представит практические решения по обеспечению защиты персональных данных в ИСПДн различных уровней сложности.

КАТАЛОГ ПРОДУКЦИИ

1. Программно-аппаратные средства для защиты информации

1.1. Средства аутентификации.

- eToken
- USB-ключ / смарт-карта eToken PRO..
- USB-ключ / смарт-карта eToken PRO (Java).
- Сертифицированные модели eToken PRO.
- Комбинированный USB-ключ eToken NG-OTP.
- Комбинированный USB-ключ eToken NG-FLASH.
- Брелок eToken PASS.

1.2. Программные средства защиты информации.

- Secret Disk.
- Secret Disk 4.
- Secret Disk Server NG.

1.3. Решения.

- eToken КРИПТО АРМ.
- eToken Windows Logon.
- eToken для Microsoft Windows 2000/XP/2003.
- eToken TMS.
- eSafe.

2. Защита рабочих станций.

- Secret Net 5.0 (автономный вариант)
- Secret Net 5.0 (мобильный вариант)
- Программно-аппаратные комплексы Аккорд
- Аккорд Nt 2000 V3.0
- Комплексы "Аккорд-1.95" и "Аккорд-NT/2000" V2.0
- Программные комплексы СЗИ НСД Аккорд
- Подсистема "Аккорд-РАУ"
- Аппаратные Модули Доверенной Загрузки

3. Защита серверов

- Сервер безопасности Secret Net 5.0
- Электронный замок Соболев

4. Защита сети

- Межсетевые экраны Check Point Firewall-1/VPN-1 5. Управление безопасностью
- Расчет комплексного управления безопасностью КУБ можно запросить у менеджера по продажам.

5. Антивирусы

- Dr.Web
- NOD32
- Антивирус Касперского

7. Сетевой сканер уязвимостей

- XSpider 7 Professional Edition(MaxPatrol 8.0)

8. Устройства гарантированного уничтожения информации на магнитных носителях

- Цунами

- Системы 2С
- Системы СТЕК
- Стек - НС1в
- Стек - НС2х
- Стек - НС2.2км

9. Оборудование для защиты помещений от утечки информации

9.1. Аппаратура защиты информации от акустической разведки

- Генератор акустического шума ЛГШ-301.
- Зашумляющая акустическая система ХАОС.
- Модели 1М аппаратуры «Соната АВ».
- Модели ДУ2mini и ДУ-К2.
- Соната - РК1
- Соната - РС1
- Соната - Р2

9.2. Защита слабых коммуникаций

- Устройство защиты Корунд.
- Устройства защиты МП.

10. Блокираторы устройств беспроводной связи

- Мозаика
- Мозаика 3ДМ
- Мозаика Интерьер
- Мозаика +
- Мозаика (i)
- Генераторы шума КМ
- КМ-3

11. Оборудование для защиты объектов вычислительной техники от утечки информации

- Генераторы пространственного зашумления
- SEL SP -21 Баррикада
- ЛГШ-501
- Контроль коммуникаций, индикаторы
- Оракул
- Оберег
- КПЛ

2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Средства аутентификации

2.1.1. **eToken** - Электронный ключ eToken - персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП) /рисунок 2.1/.



Рисунок 2.1 - Электронный ключ **eToken**

eToken выпускается в форм-факторах USB-ключа, смарт-карты или брелока. Модель eToken NG-OTR имеет встроенный генератор одноразовых паролей. Модель eToken NG-FLASH имеет встроенный модуль flash-памяти объемом до 4 ГБ. Модель eToken PASS содержит только генератор одноразовых паролей. Модель eToken PRO (Java) аппаратно реализует генерацию ключей ЭЦП и формирование ЭЦП по стандарту ГОСТ Р 34.10-2001.

Дополнительно eToken могут иметь встроенные бесконтактные радио-метки (RFID-метки), что позволяет использовать eToken также и для доступа в помещения.

Модели eToken, сертифицированные ФСТЭК России, следует использовать для **аутентификации** пользователей и хранения ключевой информации в автоматизированных системах, обрабатывающих конфиденциальную информацию, до класса защищенности 1Г включительно. Они являются рекомендуемыми носителями ключевой информации для сертифицированных СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.)

2.1.2. USB-ключ / смарт-карта eToken PRO.

USB-ключи и смарт-карты eToken PRO выполнены на базе микросхемы смарт-карты и предназначен для **аутентификации** и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП) /рисунок 2.2/.



Рисунок 2.2ю USB-ключ / смарт-карта eToken PRO

Возможные модификации:

- - по форм-фактору исполнения: USB-ключ, смарт-карта;
- - по объёму памяти смарт-карты: 32, 64 КБ;
- - сертифицированная версия (ФСТЭК России);
- - по наличию встроенной радио-метки;
- - нанесение рельефного логотипа на корпус USB-ключа, печать на поверхности смарт-карты, нанесение логотипа на корпус USB-ключа методом тампопечати;
- - по цвету корпуса для USB-ключа.

2.1.3. USB-ключ / смарт-карта eToken PRO (Java).

Новое поколение USB-ключей и смарт-карт eToken – решение компании Aladdin в сфере **аутентификации и информационной безопасности, построенное на базе Java-карты, что значительно увеличивает функциональные возможности eToken и расширяет сферу его применения.** в сфере аутентификации и информационной безопасности, построенное на базе Java-карты, что значительно увеличивает функциональные возможности eToken и расширяет сферу его применения /рисунок 2.3/.



Рисунок 2.3. USB-ключ / смарт-карта eToken PRO (Java)

eToken PRO (Java) обладает всей функциональностью eToken PRO и программно полностью с ним совместим. Дополнительно eToken o (Java) имеет увеличенный объем памяти для защищённого хранения пользовательских данных (72 КБ) и предоставляет возможность расширения функционала за счет загрузки дополнительных приложений (апплетов). eToken PRO (Java)

аппаратно реализует генерацию ключей ЭЦП и формирование ЭЦП по стандарту ГОСТ Р 34.10-2001.

Для работы USB-ключей eToken PRO (Java) в ОС Windows Vista установка драйверов не требуется (драйвера входят в состав операционной системы).

Возможные модификации:

- по форм-фактору исполнения: USB-ключ, смарт-карта;
- сертифицированная версия (ФСБ России) – на этапе сертификационных испытаний;
- по наличию встроенной радио-метки;
- нанесение рельефного логотипа на корпус USB-ключа, печать на поверхности смарт-карты, нанесение логотипа на корпус USB-ключа методом тампопечати;
- по цвету корпуса для USB-ключа.

2.1.4. Сертифицированные модели eToken PRO.

Модели eToken PRO от компании Aladdin, NG-OTP и NG-FLASH сертифицированы в **системе сертификации** средств защиты информации (ФСТЭК России), сертификат соответствия №925/5 от 05 марта 2008 г. Их следует использовать для **аутентификации** пользователей и хранения ключевой информации в автоматизированных системах, обрабатывающих **конфиденциальную информацию**, до класса защищенности 1Г включительно. Сертифицированные eToken являются рекомендуемыми носителями ключевой информации для сертифицированных СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.) /рисунок 2.4/.



Рисунок 2.4. Сертифицированные модели eToken PRO

Возможные модификации:

- по наличию встроенной радио-метки;
- нанесение рельефного логотипа на корпус USB-ключа, печать на поверхности смарт-карты, нанесение логотипа на корпус USB-ключа методом тампопечати;
- по цвету корпуса для USB-ключа.

2.1.5. Комбинированный USB-ключ eToken NG-OTP.

Комбинированный USB-ключ eToken NG-OTP – одно из решений в области информационной безопасности от компании Aladdin. Он сочетает функционал **смарт-карты** и генератора **одноразовых паролей**. Он сочетает функционал и генератора одноразовых паролей. eToken NG-OTP имеет встроенный аппаратный генератор одноразовых паролей, ЖК-дисплей для их отображения и кнопку для их генерации) /рисунок 2.4/.



Рисунок 2.4. Комбинированный USB-ключ eToken NG-OTP

Возможные модификации:

- по объёму памяти смарт-карты: 32, 64 КБ;
- сертифицированная версия (ФСТЭК России);
- по наличию встроенной радио-метки;
- по цвету корпуса.

1.1.5. Комбинированный USB-ключ eToken NG-FLASH.

Комбинированный USB-ключ eToken NG-FLASH – одно из решений в области информационной безопасности от компании Aladdin. Он сочетает функционал смарт-карты с возможностью хранения больших объёмов пользовательских данных во встроенном модуле. Он сочетает функционал смарт-карты с возможностью хранения больших объёмов пользовательских данных во встроенном модуле flash-памяти. eToken NG-FLASH также обеспечивает возможность загрузки операционной системы компьютера и запуска пользовательских приложений из flash-памяти /рисунок 2.3/



Комбинированный USB-ключ eToken NG-FLASH

Возможные модификации:

- по объёму встроенного модуля flash-памяти: 512 МБ; 1, 2 и 4 ГБ;
- сертифицированная версия (ФСТЭК России);
- по наличию встроенной радио-метки;
- по цвету корпуса.

1.1.6. Брелок eToken PASS.

eToken PASS от компании Aladdin – автономный генератор одноразовых паролей, не требующий для своей работы подключения к компьютеру. – автономный генератор одноразовых паролей, не требующий для своей работы подключения к компьютеру. eToken PASS имеет кнопку для генерации одноразовых паролей и ЖК-дисплей для их отображения /рисунок 2.3/.



Брелок eToken PASS

Возможные модификации:

- нанесение логотипа на корпус устройства методом тампопечати.

1.2. Программные средства защиты информации.

1.2.1. Secret Disk.

Secret Disk - система защиты конфиденциальной информации на персональных компьютерах и съёмных носителях от несанкционированного доступа, копирования, повреждения, кражи или изъятия. — система на персональных компьютерах и съёмных носителях от несанкционированного доступа, копирования, повреждения, кражи или изъятия.

Secret Disk с помощью самых современных технологий **шифрования** позволяет создавать на компьютере зашифрованные диски, предназначенные для безопасного хранения конфиденциальной информации. **Защита дисков** достигается за счет "прозрачного" шифрования данных - при записи на защищенный диск информация автоматически зашифровывается, при чтении - расшифровывается. Secret Disk позволяет зашифровывать разделы жёсткого диска, включая си-

стемный раздел, динамические тома и виртуальные диски, съёмные диски (дискеты, Flash-диски, SD, CF, Memory-Stick и др.), а также создавать зашифрованные файлы-контейнеры, которые монтируются в системе в виде логических дисков.

Доступ к зашифрованной информации может получить только ее владелец либо авторизованные им доверенные лица, имеющие USB ключ или смарт-карту eToken и знающие PIN-код. Для остальных зашифрованный диск выглядит как неразмеченная область жесткого диска или файл, содержащий "мусор".

Назначение:

- Защита от несанкционированного доступа и раскрытия конфиденциальной информации (коммерческой тайны, персональных данных), обрабатываемой и хранящейся на персональном компьютере или ноутбуке, когда есть риск его кражи или несанкционированного использования.

- Защита от несанкционированной загрузки ОС и получения доступа к системным файлам, файлу подкачки Windows, временным файлам приложений, файлам-журналам и другим файлам, содержащим информацию о сеансах работы пользователя, о подключениях к закрытым ресурсам, о переписке пользователя.

- Защита при несанкционированном подключении к компьютеру по сети, например, излишне любопытного системного администратора, при подключении к Интернету, когда есть риск проникновения хакеров или получения вместе с почтой "троянов" и программ-шпионов (spyware), которые могут скопировать и переслать по Сети хранящуюся на компьютере информацию.

- Персонализированный доступ и сокрытие, когда необходимо обеспечить доступ к **конфиденциальной информации** лишь одному или нескольким сотрудникам, не допустить ее попадания в чужие руки, а также скрыть сам факт наличия определенных программ и данных.

- **Защита информации** при переносе и хранении на съёмных носителях от кражи, случайной утери или при несанкционированном использовании носителей.

Создание и хранение защищенных резервных копий на CD, DVD, магнитных лентах, файловых серверах, FTP.

1.2.2. Secret Disk 4.

Secret Disk 4 - система защиты конфиденциальной информации и персональных данных, хранящихся и обрабатываемых на персональном компьютере или ноутбуке, когда есть риск его кражи, утери или несанкционированного использования.

Secret Disk 4 создает на персональном компьютере скрытые ресурсы – зашифрованные диски, предназначенные для безопасного хранения **конфиденциальной информации**.



Secret Disk 4

Защита дисков достигается за счет "прозрачного" **шифрования** данных - при записи на зашифрованный диск информация автоматически зашифровывается, при чтении - расшифровывается.

Доступ к зашифрованной информации может получить только ее владелец либо авторизованные им доверенные лица, имеющие электронный ключ eToken и знающие PIN-код.

Для других пользователей этот зашифрованный ресурс будет не виден и недоступен. Более того, они могут даже и не догадываться о его наличии. В отключенном состоянии зашифро-

ванный диск выглядит как неразмеченная область жесткого диска или файл, содержащий "мусор".

Основные возможности системы:

- **Шифрование** системного раздела, разделов на жестких дисках, томов на динамических дисках, виртуальных дисков и съемных носителей.
- **Аутентификация** пользователя по USB-ключу eToken для загрузки операционной системы и для доступа к зашифрованным данным.
- **Запрет доступа по сети** к зашифрованным данным для всех пользователей, включая системного администратора.
- **Восстановление доступа** к данным в случае утери USB-ключа.
- **Защита данных от сбоев** во время операций шифрования, включая перебои электропитания.

Режим энергосбережения для ноутбуков.

1.2.3. Secret Disk Server NG.

Secret Disk Server NG - система защиты корпоративных баз и конфиденциальных данных на серверах от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия. - система на серверах от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия.

Secret Disk Server NG создает на сервере скрытые ресурсы – **зашифрованные диски**, предназначенные для безопасного хранения конфиденциальной информации.



Secret Disk Server NG

Защита информации осуществляется методом "**прозрачного**" шифрования с помощью стойких алгоритмов шифрования: при записи на зашифрованный диск информация автоматически зашифровывается, при чтении - расшифровывается. Зашифровать можно отдельные жесткие диски сервера, любые дисковые массивы (внешние и внутренние, программные и аппаратные RAID-массивы), а также съемные диски (например, подключаемые к серверу для резервного копирования).

Находящиеся на диске данные всегда зашифрованы, что делает доступ к ним невозможным для злоумышленника даже в случае кражи или изъятия как отдельного диска, так и всего сервера. В отключенном состоянии зашифрованный диск выглядит как неразмеченная область жесткого диска или файл, содержащий "мусор".

Основные возможности системы:

- **Шифрование** разделов на жестких дисках, томов на динамических дисках, съемных носителей, создание виртуальных зашифрованных дисков.
- Использование **стойких алгоритмов шифрования**, возможность подключения внешних криптовайдеров КриптоПро CSP, Signal-COM CSP и Infotecs CSP, реализующих ГОСТ 28147-89 с длиной ключа 256 бит.
- **Удаленное** и групповое **администрирование** Secret Disk Server NG выполняется через консоль управления Microsoft или удаленный рабочий стол.
- **Защита данных от сбоев** во время операций шифрования, включая перебои электропитания.
- Поддержка Volume Shadow Copy для платформы Windows Server 2003.

Интеграция с модулем подачи сигнала "тревога".

1.3 Решения.

1.3.1. eToken КРИПТО АРМ.

eToken КРИПТОАРМ – эффективный инструмент обеспечения **информационной безопасности** - обеспечивает комплексное решение технических вопросов организации защищённого юридически значимого электронного документооборота на корпоративном уровне. Решение предназначено для использования в государственном и коммерческом секторах рынка.



eToken КРИПТО АРМ

Состав решения:

КРИПТОАРМ Стандарт (разработчик – компания [Digit](#)) – программа, предназначенная для **шифрования** и **электронной цифровой подписи (ЭЦП)** документов, передаваемых по незащищенным каналам связи (Интернету, электронной почте) и на съемных носителях. При выполнении перечисленных операций «КРИПТОАРМ» использует функции криптопровайдера КриптоПро CSP.

СКЗИ КриптоПро CSP (разработчик – компания «[КРИПТО-ПРО](#)») – сертифицированное средство криптографической защиты информации, предназначенное для **авторизации** и обеспечения контроля подлинности электронных документов при обмене ими между пользователями с применением ЭЦП; обеспечения конфиденциальности и контроля целостности информации посредством ее **шифрования** и имитозащиты и др.

Электронный ключ eToken PRO (разработчик – компания [ЗАО «Аладдин Р.Д.»](#)) – сертифицированное средство **аутентификации** пользователя и хранения личных данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП. Предназначен для защищённого хранения ключевой информации пользователя (закрытые ключи ЭЦП), а также сертификатов открытого ключа

Основные возможности:

- строгая аутентификация на базе цифровых сертификатов (гибкая настройка доступа и защита от несанкционированных действий с закрытыми данными конечных пользователей)
- контроль целостности электронных документов при обмене ими между пользователями с применением ЭЦП
- гарантия авторства электронных документов с использованием ЭЦП
- неотказуемость пользователя от выполненных действий (соблюдение обязательств со стороны участников документооборота)
- защита от НСД, кражи и использования как отдельных файлов, так и любой информации, хранящейся в базах данных

Комплексный продукт может использоваться :

- для организации рабочего места в РКІ
- в качестве основы для встраивания криптографии в бизнес-системы

1.3.2. eToken Windows Logon.

eToken Windows Logon – решение в области **информационной безопасности и аутентификации** предназначен для кардинального решения проблемы "слабых" паролей при работе на компьютерах под управлением Microsoft Windows. Сразу после установки продукта для входа на компьютер или в сеть можно начать использовать надёжные и стойкие к перебору пароли, либо цифровые сертификаты.



eToken Windows Logon

eToken Windows Logon сгенерирует сложный пароль, установит его в системе и сохранит в памяти eToken. Пользователю не нужно запоминать новый пароль – достаточно при входе на компьютер подключить eToken и ввести его PIN-код – хранящийся в памяти пароль будет передан в систему. Таким образом, пароль не надо запоминать и вводить с клавиатуры – это исключает возможность его подсматривания или перехвата злоумышленником.

eToken Windows Logon значительно снижает влияние "человеческого фактора" на уровень безопасности Windows. Внедрение и правильное использование продукта позволят исключить возможность обращения злоумышленников к ресурсам системы от имени легальных пользователей.

eToken Windows Logon обеспечивает: обеспечивает:

- **аутентификацию** пользователей на компьютере и в сети Microsoft Windows с помощью USB-ключей или смарт-карт eToken;
 - использование регистрационных имён и паролей при **авторизации** для локального входа в систему или для входа в домен;
 - использование цифровых сертификатов X.509, сертификатов пользователя со смарт-картой и закрытых ключей для входа в домен;
 - генерирование и последующее применение случайных паролей, неизвестных пользователю;
- возможности однофакторной (eToken) и двухфакторной (eToken + PIN-код) аутентификации.

1.3.3. eToken для Microsoft Windows 2000/XP/2003.

eToken для Microsoft Windows 2000/XP/2003 обеспечивает строгую двухфакторную **аутентификацию** пользователей при входе в сеть Microsoft Windows и службу каталога Microsoft Active Directory на основе цифровых сертификатов стандарта X.509. Функции центра сертификации (CA) выполняет служба сертификатов, входящая в состав серверов Microsoft Windows. Решение поддерживает технологию Windows Single Sign-On, которая обеспечивает единую регистрацию пользователя и устраняет необходимость дополнительной регистрации в каждом из используемых приложений, повышая тем самым **информационную безопасность**.

eToken используется для генерации ключевых пар RSA (открытый и закрытый ключи), выполнения криптографических операций с закрытым ключом в доверенной среде (например, формирование ЭЦП), а также надёжного хранения цифровых сертификатов и ключевой информации. eToken совместим с продуктами PKI ведущих мировых и отечественных производителей - Baltimore, CA eTrust, Entrust, Microsoft CA, RSA Keon, "Удостоверяющий Центр" Крипто-Про.



eToken для Microsoft Windows 2000/XP/2003

eToken для Microsoft Windows 2000/XP/2003 предназначен для:

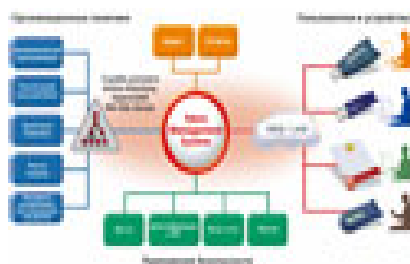
- усиления функций безопасности ОС Microsoft Windows 2000/XP/2003 за счёт полного отказа от парольной аутентификации в пользу строгой двухфакторной аутентификации (по смарт-картам / USB-ключам eToken);
- обеспечения конфиденциальности и целостности электронной корреспонденции и офисных документов за счёт использования ЭЦП и шифрования данных;
- повышения безопасности виртуальных частных сетей, построенных на платформе Microsoft Windows 2000/XP/Server 2003;
- обеспечения безопасного подключения к удалённому рабочему столу Windows XP или Windows Server 2003;

усиления защиты веб-серверов на платформе Microsoft Internet Information Services, подключение к которым осуществляется по протоколу HTTPS.

1.3.4. eToken TMS.

eToken TMS (Token Management System) – система, предназначенная для централизованного управления и ведения учета персональных аппаратных и программных средств **аутентификации** и хранения ключевой информации (USB-ключей и смарт-карт eToken) в масштабах предприятия в целях его информационной безопасности.

eToken TMS является связующим звеном между пользователями, средствами аутентификации, приложениями информационной безопасности и установленными на предприятии политиками безопасности (организационными правилами и регламентами).



eToken TMS

Основные возможности системы:

- **Поэкземплярный учет и регистрация** всех аппаратных и программных средств аутентификации и хранения ключевой информации, используемых сотрудниками.
- **Ускорение ввода в эксплуатацию** электронных ключей и смарт-карт, автоматизация процессов выдачи eToken сотруднику, персонализация eToken, запись ключевой информации и аутентификационных данных в память устройства.

- **Управление жизненным циклом** средств аутентификации и хранения ключевой информации:

- обновление аутентификационных данных и ключевой информации,
- предоставление / отзыв прав доступа к приложениям при изменении служебных обязанностей / увольнении сотрудника,
- замена устройства при его утере / повреждении,
- вывод устройства из эксплуатации.

- **Аудит использования** сотрудником выданного ему средства аутентификации и хранения ключевой информации – фиксируются все факты использования устройства сотрудником на компьютерах предприятия, изменения хранящихся в памяти устройства данных.

Подготовка отчетов для руководителей служб ИТ и ИБ об использовании сотрудниками средств аутентификации и хранения ключевой информации (на основе данных аудита средствами встроенного Ггенератора отчетов, также имеется возможность экспорта данных во внешние средства построения отчетов).

для руководителей служб ИТ и ИБ об использовании сотрудниками средств аутентификации и хранения ключевой информации (на основе данных аудита средствами встроенного Ггенератора отчетов, также имеется возможность экспорта данных во внешние средства построения отчетов).

eSafe.

eSafe -система комплексного обеспечения проактивной безопасности информации в корпоративной сети на уровне Интернет-шлюзов и почтовых серверов. eSafe способен обнаруживать неразрешенные к использованию приложения, надежно блокировать программы-шпионы на каждом компьютере сети, а также эффективно противодействовать вирусным атакам, осуществлять потоковую фильтрацию и очистку почтового и Интернет-трафиков.

Данный комплекс свободно интегрируется в любую корпоративную сеть и бесперебойно работает вместе с любыми решениями сторонних производителей, обеспечивающих комплексную **безопасность сети**.

Сфера использования – Основными потребителями являются **средние и крупные компании, MSP и ISP провайдеры, а также операторы мобильной связи**, предоставляющие услуги доступа в Интернет.

Решение представлено как программное, так и аппаратное.

Модельный ряд eSafe включает в себя:

- **eSafe Mail – это решение для почтовых серверов, позволяющее обеспечить безопасность почтового трафика (защита от спама, вредоносного кода, хакерских атак) благодаря использованию репутационного и контентного фильтров. eSafe Mail может использоваться в связке с другими решениями eSafe, предотвращая возможность проникновения любых типов вредоносного контента по протоколам SMTP, POP3, через Webmail или HTML в теле email.** – это решение для почтовых серверов, позволяющее обеспечить безопасность почтового трафика (защита от , вредоносного кода, хакерских атак) благодаря использованию репутационного и контентного фильтров. eSafe Mail может использоваться в связке с другими решениями eSafe, предотвращая возможность проникновения любых типов вредоносного контента по протоколам SMTP, POP3, через Webmail или HTML в теле email.

- **eSafe Web – это решение для фильтрации трафика предприятия.** – это решение для фильтрации трафика предприятия. eSafe Web предоставляет защиту сети от вредоносного кода, шпионских приложений; использует уникальную технологию (NitroInspection) проверки «на лету» HTTP и FTP трафиков, а также единственное решение (AppliFilter) , предназначенное для блокирования угроз на уровне приложений (IM, p2p).

- **eSafe Web SSL – это решение, предназначенное для сканирования трафика в защищенных протоколах.** – это решение, предназначенное для сканирования трафика в защищенных протоколах.

eSafe Gateway– это совокупность решений eSafe Mail+eSafe Web, предназначенная для предотвращения проникновения в защищаемую сеть известных и неизвестных вредоносных программ, спама, и ограничивающее доступ к данным, не соответствующим корпоративной политике или морально-этическим нормам.– это совокупность решений , предназначенная для предотвращения проникновения в защищаемую сеть известных и неизвестных вредоносных программ, спама, и ограничивающее доступ к данным, не соответствующим корпоративной политике или морально-этическим нормам.

2. ЗАЩИТА РАБОЧИХ СТАНЦИЙ

- 2.1. Secret Net 5.0 (автономный вариант)
- 2.2. Secret Net 5.0 (мобильный вариант)
- 2.3. Программно-аппаратные комплексы Аккорд
 - 2.3.1. Аккорд Nt 2000 V3.0
 - 2.3.2. Комплексы "Аккорд-1.95" и "Аккорд-NT/2000" V2.0
- 2.4. Программные комплексы СЗИ НСД Аккорд
- 2.5. Подсистема "Аккорд-РАУ"
- 2.6. Аппаратные Модули Доверенной Загрузки

2.1. Secret Net 5.0 (автономный вариант).

Защитные механизмы системы можно условно разделить на следующие группы

- Авторизация пользователей
- Разграничение доступа
- Защита информации в процессе хранения
- Контроль отчуждаемой информации

2.1.1. Авторизация пользователей

Идентификация и аутентификация пользователей. Система Secret Net 5.0 совместно с ОС Windows обеспечивает идентификацию и аутентификацию пользователя с помощью средств аппаратной поддержки при его входе в систему. В качестве аппаратной поддержки система Secret Net 5.0 использует: программно-аппаратный комплекс «Соболь», Secret Net Touch Memory Card. В качестве устройств ввода идентификационных признаков используются:

- iButton;
- eToken R2;
- Proximity Card.

Защита от загрузки с внешних носителей. С помощью средств аппаратной поддержки существует возможность запретить обычному пользователю загрузку ОС с внешних съёмных носителей.

Также, плату аппаратной поддержки невозможно обойти средствами BIOS: если в течение определённого времени после включения питания на плату не было передано управление, она блокирует работу всей системы.

2.1.2. Разграничение доступа

Полномочное управление доступом. Выполняет функцию управления доступом пользователей к конфиденциальной информации. Каждому пользователю и каждому информационному ресурсу назначается один из трёх уровней конфиденциальности: “Не конфиденциально”, “Конфиденциально”, “Строго конфиденциально”. Доступ осуществляется по результатам сравнения уровня допуска в соответствии с категорией конфиденциальности, присвоенной информации, и уровнем допуска пользователя к конфиденциальной информации.

Разграничение доступа к устройствам. Обеспечивает разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера. Разграничивается доступ к следующим портам/устройствам:

- последовательные и параллельные порты;
- сменные, логические и оптические диски.
- USB – порты, IrDA, WiFi – подключения.

Замкнутая программная среда. Для каждого пользователя компьютера формируется определённый перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей. Применение этого режима позволяет исключить распространение вирусов, «червей» и шпионского ПО.

2.1.3. Защита информации в процессе хранения

Контроль целостности. Используется для слежения за неизменностью контролируемых объектов с целью защиты их от модификации. Контроль проводится в автоматическом режиме в соответствии с некоторым заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков. Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие файлов по заданному пути. При обнаружении несоответствия предусмотрены следующие варианты реакции на возникающие ситуации нарушения целостности:

- регистрация события в журнале Secret Net;
- блокировка компьютера;
- восстановление повреждённой/модифицированной информации;
- отклонение или принятие изменений.

Шифрование файлов. Предназначено для усиления защищенности информационных ресурсов компьютера. В системе Secret Net 5.0 управление шифрованием файлов и доступ к зашифрованным файлам осуществляется на уровне каталога. Пользователь, создавший зашифрованный ресурс, является его владельцем, он может пользоваться им индивидуально и предоставлять доступ к этому ресурсу другим пользователям. Шифрование файлов производится по алгоритму ГОСТ 28147-89.

Гарантированное уничтожение данных. Уничтожение достигается путем записи случайной последовательности на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено несколько циклов (проходов) затирания.

Контроль аппаратной конфигурации компьютера. Осуществляет своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирования на эти изменения.

Предусмотрено два вида реакций:

- регистрация события в журнале Secret Net;
- блокировка компьютера.

2.1.4. Контроль над отчуждаемой информацией

Контроль печати конфиденциальной информации. Печать осуществляется под контролем системы защиты. При разрешённом выводе конфиденциальной информации на печать документы автоматически маркируются в соответствии с принятыми в организации стандартами. Также факт печати отображается в журнале защиты Secret Net 5.0.

Регистрация событий. Система Secret Net 5.0 регистрирует все события, происходящие на компьютере:

- включение \ выключение компьютера,
- вход \ выход пользователей,
- события НСД,
- запуск приложений,
- обращения к конфиденциальной информации,
- контроль вывода конфиденциальной информации на печать и отчуждаемые носители и

т.п.

А также...

Функциональный самоконтроль подсистем. Самоконтроль производится перед входом пользователя в систему и предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 5.0 загружены и функционируют.

Импорт и экспорт параметров. В Secret Net 5.0 реализована возможность экспорта и импорта различных параметров системы. После проверки корректности работы защитных меха-

низмов на компьютере, принимаемом за эталонный, выполняется экспорт значений параметров в файл. Далее значения импортируются на необходимое количество компьютеров.

2.2. Secret Net 5.0 (мобильный вариант).

Это - система защиты информации от несанкционированного доступа для мобильных компьютеров. Она реализует требования руководящих документов и ГОСТ по защите информации, не ограничивая возможности ОС и прикладного программного обеспечения.

Он - позволяет защитить конфиденциальную информацию от несанкционированного доступа вне зависимости от того, где и в каком качестве используется ноутбук – при работе во внутренней сети организации или в дальней командировке.

Это - программное решение, который обеспечивает защиту мобильных ПК, работающих под управлением операционных систем Windows 2000, Windows XP и Windows 2003.

Достоинства

- Работает совместно с ОС Windows, расширяя, дополняя и усиливая стандартные механизмы защиты;
- Обеспечивает разграничение доступа к конфиденциальной информации на мобильных ПК;
- Контролирует наиболее критичные каналы распространения конфиденциальной информации;
- Поддерживает работу с аппаратными идентификаторами eToken;
- Обеспечивает шифрование особо важных сведений;
- Сертификат ФСТЭК № [1119](#) позволяет применять Secret Net 5.0 (мобильный вариант) для защиты конфиденциальной информации.

Возможности. Secret Net 5.0 (мобильный вариант) является, по сути, облегчённой версией Secret Net 5.0 (автономный вариант) . Основное отличие состоит в отсутствии необходимости применения платы аппаратной поддержки.

2.3. Программно-аппаратный комплекс Аккорд

2.3.1. Аккорд Nt 2000 V3.0

Программно-аппаратный комплекс средств защиты информации (ПАК СЗИ) Аккорд-NT/2000 V3.0 предназначен для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам.

Комплекс работает

- на всей ветви операционных систем (ОС) Microsoft NT +,
- на терминальных серверах, построенных на базе ОС Windows 2000 Advanced Server и
- на базе серверов семейства Windows 2003, и
- ПО Citrix Metaframe XP, работающем на этих ОС.

Комплекс использует собственную систему разграничения доступа (мандатный и дискреционный методы контроля) и служит фильтром между ядром ОС и расположенным выше прикладным ПО терминальных служб. В нем действия, разрешенные прикладным ПО, но запрещенные АККОРДОМ - будут запрещены пользователю.

Комплексная защита терминальной сессии обеспечивается тогда и только тогда, когда пользователь может работать только с защищенного терминала и только с защищенным терминальным сервером. Для этого в момент создания терминальной сессии со стороны терминального сервера необходимо аутентифицировать не только пользователя, но и терминал, а со стороны терминала необходимо убедиться в том, что терминальный сервер действительно тот, с которым должен работать пользователь. Это возможно только при наличии активных СЗИ и на терминале, и на сервере.

Стало быть, для защиты терминальной сессии необходимо установить комплекс не только на терминальный сервер, но и на терминалы.

В предлагаемой системе защиты терминальных сессий комплексы Аккорд, установленные на терминальных серверах и на пользовательских терминалах, взаимодействуют в рамках виртуальных каналов, построенных на протоколах RDP и ICA. Это позволяет использовать уже установленную связь между сервером и терминалом, а не устанавливать новую.

При этом состав полномочий пользователя инвариантен как к протоколу подключения, так и к типу терминального сервера (Microsoft или Citrix).

Комплекс характеризуется также набором возможностей, добавленных к функциям классической версии ПАК Аккорд-NT/2000 V2.0:

- усиленная аутентификация терминальных станций с помощью контроллера Аккорд или ПСКЗИ ШИПКА,

- идентификация/аутентификация пользователей, подключающихся к терминальному серверу (с использованием ТМ-идентификатора или ПСКЗИ ШИПКА),

- опциональная автоматическая идентификация в системе Windows NT+ и на терминальном сервере пользователей, аутентифицированных защитными механизмами контроллера АМДЗ (при таком подходе, избегая повторной идентификации пользователей, можно гарантировать, что ОС будет загружена под именем того же пользователя, который был аутентифицирован в контроллере АМДЗ, и к терминальному серверу подключится тот же самый пользователь).

- управление терминальными сессиями,

- контроль печати на принтерах, подключенных как к терминальным серверам, так и к пользовательским терминалам, который позволяет протоколировать вывод документов на печать и маркировать эти документы (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

В течение всего сеанса работы пользователя ведется подробный журнал событий, в котором фиксируются все действия пользователя на терминальном сервере.

На основании результатов сертификационных испытаний получен сертификат соответствия [№ 1161](#), удостоверяющий, что комплекс Аккорд-NT/2000 V3.0 может применяться на объектах информатизации **второй категории**.

2.3.2. Комплексы "Аккорд-1.95" и "Аккорд-NT/2000" V2.0

Комплексы "Аккорд-1.95" и "Аккорд-NT/2000" V2.0 обеспечивают защиту от несанкционированного доступа к ПЭВМ и информации для

- автономных ПЭВМ и

- сетей с применением персональных идентификаторов пользователей, выполненных на базе устройств iButton и смарт-карт.

В основе комплексов - "Аккорд-АМДЗ" (на базе контроллеров "Аккорд-4++", "Аккорд-4.5", "Аккорд-5", "Аккорд-PC104", "Аккорд-СБ", "Аккорд-МХ", "Аккорд-5.5", "Аккорд-Mini-PCI") и специальное программное обеспечение, реализующее правила разграничения доступа к информации (в "Аккорд-1.95" - для операционных систем MS DOS, Windows 9x, Windows Millenium, а в "Аккорд-NT/2000" V2.0 - для Windows NT, Windows 2000, Windows XP, Windows 2003).



"Аккорд-1.95" и "Аккорд-NT/2000" V2.0 обеспечивают:

- защиту от несанкционированного доступа к ПЭВМ;
- идентификацию/ аутентификацию пользователей до загрузки операционной системы с последующей передачей результатов успешной идентификации/аутентификации в операционную систему;
- аппаратный контроль целостности системных файлов и критичных разделов реестра;
- доверенную загрузку ОС;
- контроль целостности программ и данных, их защиту от несанкционированных модификаций;
- создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
- запрет запуска неразрешенных программ;
- разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
- разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
- автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса.

Программное обеспечение комплексов позволяет администратору безопасности информации описать **любую не противоречивую политику безопасности** на основе наиболее полного набора атрибутов (табл. 2.1).

Таблица 2.1. – Набор атрибутов

Операции с файлами	
R	разрешение на открытие файлов только для чтения
W	разрешение на открытие файлов для записи
C	разрешение на создание файлов на диске
D	разрешение на удаление файлов
N	разрешение на переименование файлов
V	видимость файлов
O	эмуляция разрешения на запись информации в открытый файл
Операции с каталогами	
M	создание каталогов на диске
E	удаление каталогов на диске
G	разрешение перехода в этот каталог
n	переименование подкаталогов
S	наследование прав на все вложенные подкаталоги
l	наследование прав на l уровень вложенности
0	запрет наследования прав на все вложенные подкаталоги
Прочее	
X	разрешение на запуск программ
Регистрация	
r	регистрация в журнале операций чтения при обращении к объекту
w	регистрация в журнале операций записи при обращении к объекту

Для разграничение прав доступа к информационным ресурсам, кроме дискреционного, осуществлен мандатный принцип доступа субъектов к информационным ресурсам.

Кроме этого, администратор БИ для каждого субъекта - пользователя системы определяет:

- перечень файлов, целостность которых должна контролироваться системой и опции контроля;
- запуск стартовой задачи (для функционально замкнутых систем);
- наличие, либо отсутствие привилегий супервизора;
- детальность журнала доступа;
- назначение/изменение пароля для аутентификации;

- временные ограничения - время по дням недели (с дискретностью 30 мин), в которое разрешено начало работ для данного субъекта;

- параметры управления экраном - гашение экрана через заранее определенный интервал времени (в случае, если в течение указанного интервала действия оператором не выполнялись), подача соответствующих звуковых и визуальных сигналов.

ПО Аккорд-NT/2000 имеет интерфейс подключения внешних антивирусных модулей. В качестве такого модуля может применяться Антивирусное ядро Vba32, разработанное фирмой ВирусБлокАда, или Антивирусное ядро DrWeb.

Совместная работа Аккорд-NT/2000 и антивирусного ядра позволяет

- не только добавить в ПО Аккорд-NT/2000 **новую функцию обнаружения и обезвреживания вредоносных программ** (при этом динамически проверяются только те объекты, к которым обращается пользователь),

- но и **существенно ускорить работу за счёт исключения дублирования проверок** (проверки производятся одновременно, а не последовательно, соответственно каждый объект проверяется единожды).

В Аккорд-NT/2000 **реализована возможность контроля доступа к USB-устройствам и контроля печати на принтерах, который позволяет протоколировать вывод документов на печать и маркировать эти документ**. В качестве маркера может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация.

Комплексы прошли испытания на соответствие требованиям РД Гостехкомиссии РФ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", их надежность подтверждена широкой практикой его внедрения и [различными Российскими сертификатами соответствия](#). Производство осуществляется на предприятии соответствующем требованиям [ISO 9001-2001 \(№ РОСС RU.0001.13ИС72 от 23.07.04 г.\)](#).

Таблица 1. – Основные характеристики комплексов "Аккорд-1.95" и "Аккорд-NT/2000" V2.0

	"Аккорд-1.95"	"Аккорд-NT/2000" V2.0
Работа под операционными системами	MS DOS, Windows 9x, Windows Millenium	Windows NT, все версии Windows 2000, Windows XP
Класс защиты	до 1В включительно	до 1В включительно
Наличие сертификата Гостехкомиссии России	№ 153/6 24 июля 2002 г.	№ 600 1 апреля 2002 г.
Используемые контроллеры	"Аккорд-4++", "Аккорд-4.5", "Аккорд-5", "Аккорд-PC104", "Аккорд-СБ/2".	
Идентификация (тип идентификатора)	Touch memory DS-199x.	Touch memory DS-199x.
Аутентификация пользователя	по паролю, вводимому с клавиатуры	по паролю, вводимому с клавиатуры

2.4. СЗИ НСД Аккорд-АМДЗ

СЗИ НСД Аккорд-АМДЗ – это аппаратный модуль доверенной загрузки (АМДЗ) для IBM-совместимых ПК – серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от несанкционированного доступа.

«**Доверенная загрузка**» – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

Комплекс начинает работу сразу после выполнения штатного BIOS компьютера – до загрузки операционной системы, и обеспечивает доверенную загрузку ОС, поддерживающих файловые системы FAT 12, FAT 16, FAT 32, NTFS, HPFS, EXT2FS, EXT3FS, FreeBSD, Sol86FS, QNXFS, MINIX.

Это, в частности, ОС семейств MS DOS, Windows (Windows 9x, Windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista), QNX, OS/2, UNIX, LINUX, BSD и др.

Аккорд-АМДЗ может быть реализован в 5 основных вариантах:

- Аккорд-5 (для шинного интерфейса PCI),
- унифицированный контроллер для шин PCI и PCI-X – Аккорд-5MX,
- его функциональный аналог в стандарте mini-PCI – Аккорд-5MX mini-PCI,
- унифицированный контроллер (PCI, PCI-X) [Аккорд-5.5](#), имеющий мощную аппаратно реализованную криптографическую подсистему, и
- его версия для шины PCIe – [Аккорд-5.5.e](#).

Контроллеры могут быть оснащены интерфейсом блокировки двух и более физических каналов (FDD, HDD (IDE), ATX, EATX). В Аккорд-5.5 также реализована возможность отключения питания компьютера в случае, если за N секунд не начал работу BIOS АМДЗ. Аккорд-АМДЗ позволяет использовать для идентификации пользователей смарт-карты, устройства iButton, устройства считывания отпечатков пальцев, а также устройство ШИПКА.

Комплекс применим для построения систем защиты информации от несанкционированного доступа в соответствии с руководящими документами ФСТЭК (Гостехкомиссии) России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» – **по 3 уровню контроля**, «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» **по классу защищенности 1Д**, и для использования в качестве средства идентификации/аутентификации пользователей, контроля целостности программной и аппаратной среды ПЭВМ (РС) при создании автоматизированных систем, удовлетворяющих требованиям руководящего документа ФСТЭК (Гостехкомиссии) России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» **до класса 1Б включительно**.

2.5. Подсистема "Аккорд-РАУ"

Подсистема "Аккорд-РАУ" - это ПО для автоматизации управления защитой информации в АС. Она объединяет Автоматизированное рабочее место администратора безопасности информации (АРМ АБИ) и пользовательские терминалы, оснащенные СЗИ семейства "АККОРД".

Построена подсистема "Аккорд-РАУ" на основе комплекса "Аккорд-AcXNet", обеспечивающего защищенный обмен данными по сети и работу специального ПО АРМ АБИ (при наличии на АРМ АБИ и рабочих станциях комплексов "Аккорд-АМДЗ" и ПО - для рабочих станций - ПО "Аккорд-1.95" или "Аккорд-NT/2000", для серверов - ПО "Аккорд-NT/2000" - является техническим условием применения подсистемы "Аккорд-РАУ", и в поставку этого продукта данные компоненты не входят!).

Оперативное наблюдение и управление

В рамках оперативного наблюдения за работой пользователя можно

- получать информацию о том, кто работает на данной станции, о версии ОС, под управлением которой идет работа, о списке задач, которые выполняются на этой станции в текущий момент времени;
- просматривать все события подсистемы разграничения доступа со всех станций в одном окне;
- при необходимости детального анализа работы одной станции, получать все поступающие события в отдельное окно;
- выбирать для просмотра только те рабочие станции или только те события, которые в данный момент представляют особенный интерес;
- оперативно изменять уровень детальности журнала на рабочих станциях;
- просматривать экран выбранной рабочей станции;
- просматривать диски рабочих станций (до уровня файлов).

Оперативное управление работой пользователя – это возможность

- посылать пользователю сообщения;
- обмениваться с пользователем файлами;
- включать пользователю Screensaver, который может быть разблокирован только ТМ-идентификатором АБИ;
- управлять «мышью» и клавиатурой рабочих станций;
- перегружать рабочие станции.

Удаленное администрирование

Централизованный сбор журналов регистрации СЗИ НСД Аккорд подразумевает

- получение журналов подсистемы разграничения доступа с рабочих станций;
- получение журналов контроллеров АМДЗ с рабочих станций;
- осуществление очистки журналов регистрации.

Администратор безопасности информации может настроить параметры сбора журналов

- с выбранных рабочих станций;
- систематизировано по соответствующим каталогам с делением по датам сбора.

Работа со списком зарегистрированных рабочих станций –

- редактирование списка станций на АРМ;
- рассылка обновленного списка по рабочим станциям.

Работа с базами пользователей и файлами конфигурации на рабочих станциях включает

- получение файлов конфигурации с выбранной станции;
- редактирование и замену файлов конфигурации выбранной станции;
- редактирование базы пользователей рабочих станций на АРМ;
- удаление пользователей станции или изменение настроек их полномочий;
- добавление новых пользователей станции и назначение им полномочий;
- синхронизация баз пользователей на рабочих станциях (в том числе, находящиеся в контроллерах)
- сразу после изменения базы или в момент начала работы рабочей станции.

2.6. Аппаратные Модули Доверенной Загрузки

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа - модуль доверенной загрузки (МДЗ) операционной системы Microsoft Windows XP Professional "Аккорд-ХР" предназначен для применения на ПЭВМ (рабочих станциях ЛВС) типа IBM PC, функционирующих под управлением ОС Microsoft Windows XP Professional (Service Pack 1a). Данная операционная система была разработана совместно компаниями Microsoft и Алтэкс Строй и сертифицирована как программный продукт общего назначения со встроенными средствами защиты от несанкционированного доступа к конфиденциальной информации.

В состав комплекса входят:

- специализированный контроллер "Аккорд-TINY" с шинным интерфейсом PCI (напряжение питания шины 3.3 или 5 вольт);
- специальное программное обеспечение для управления списком контролируемых объектов в среде ОС Windows XP.

Контроллер "Аккорд-TINY" обеспечивает:

- блокировку загрузки ПЭВМ с отчуждаемых носителей (FDD, CD ROM, ZIP Drive, USB флэш-диск);
- контроль целостности программ, данных и системных областей жестких дисков, а также конфигурации технических средств ПЭВМ (PC);
- хранение списка контролируемых объектов и журнала регистрации событий во внутренней энергонезависимой памяти;

- возможность изменения встроенного ПО контроллера (технологический режим) без замены аппаратной части комплекса;
- на аппаратном уровне режим доверенной загрузки сертифицированных версий ОС Windows XP (выполнение процедур контроля целостности системных разделов диска, программ, данных и ключей реестра).

Под термином "доверенная загрузка" понимается загрузка ОС только после проведения процедур проверки целостности технических и программных средств ПЭВМ с использованием алгоритма пошагового контроля целостности. Комплекс "Аккорд-ХР" работает с файловыми системами FAT 16, FAT 32, NTFS.

Специальное программное обеспечение устанавливается на жесткий диск ПЭВМ и предназначено для:

- формирования и редактирования списка контролируемых объектов;
- расчета контрольных сумм;
- записи данных в энергонезависимую память аппаратной части комплекса (МДЗ);
- просмотра журнала регистрации событий, возникающих в процессе работы МДЗ.

Комплекс "Аккорд-ХР" имеет сертификат Государственной технической комиссии при Президенте Российской Федерации № 938 от 29 сентября 2004 г., как программно-техническое средство защиты от несанкционированного доступа к конфиденциальной информации, обрабатываемой в ОС Windows XP.

3. ЗАЩИТА СЕРВЕРОВ

3.1. Сервер безопасности Secret Net 5.0

3.2. Электронный замок Соболев

3.1. Сервер безопасности Secret Net 5.0

– это система защиты конфиденциальной информации от несанкционированного доступа, которая функционирует под управлением современных ОС MS Windows 2000, Windows XP и Windows 2003.

– это комплексное решение, которое сочетает в себе большой набор функциональных возможностей по защите информации, средства централизованного управления настройками защитных механизмов, средства оперативного реагирования на действия инсайдеров и возможность мониторинга безопасности защищаемой информационной системы в режиме реального времени.

Достоинства решения

За счёт тесной интеграции собственных защитных механизмов с механизмами управления сетевой инфраструктуры защищаемой сети, Secret Net 5.0 повышает защищенность всей автоматизированной информационной системы компании в целом:

- Обеспечивает централизованное управление настройками политики безопасности;
- Работает совместно с ОС Windows, расширяя, дополняя и усиливая стандартные механизмы защиты;
- Осуществляет мониторинг и аудит политики безопасности в режиме реального времени;
- Позволяет оперативно реагировать на события НСД;
- Поддерживает терминальный режим работы пользователей с рабочей станцией.

Глубокая интеграция системы управления Secret Net 5.0 со штатными механизмами управления информационной системой позволяет избежать постоянно возникающих проблем синхронизации данных между ИС и выделенным сервером настроек, который имелся в предыдущих версиях системы и часто присутствует в аналогичных системах защиты.

Основные возможности

- Централизованное управление
- Оперативное реагирование на действия злоумышленников
- Централизованный просмотр событий безопасности
- Контроль вывода конфиденциальной информации на внешние носители
- Аппаратная идентификация пользователей

- Контроль целостности файлов
- Разграничение доступа к устройствам (CD\DVD, USB, Wi-Fi и т.д.)

3.2. Электронный замок Соболев

Устройство "Соболев" является электронным замком. Его назначение - предотвращать доступ посторонних лиц к информации, хранящейся на компьютере, и регистрировать попытки доступа к компьютеру.

Электронный замок "Соболев" может использоваться, если компьютер работает под управлением следующих операционных систем:

- DOS 6.22,
- Windows 95,
- Windows 98,
- Windows NT 4.0,
- Windows 2000,
- Windows XP,
- Windows 2003.

Четыре основных достоинства электронного замка "Соболев"

- **Наличие сертификатов** ФАПСИ и Гостехкомиссии России
- Защита информации, составляющей государственную тайну
- Помощь в построении прикладных криптографических приложений
- Простота в установке, настройке и эксплуатации

Четыре основных возможности

- Идентификация пользователей по электронным идентификаторам
- Защита операционной системы от модификации
- Проверка целостности операционной системы и данных на жестком диске
- Регистрация несанкционированных действий

4. ЗАЩИТА СЕТИ

Межсетевые экраны Check Point Firewall-1/VPN-1

Межсетевые экраны Check Point NG, разработанной израильской компанией Check Point Software Technologies, позволяют эффективно решить задачи разграничения доступа к ресурсам корпоративной сети внешних пользователей и защиты информационного взаимодействия с ними.

Разнообразные варианты применения позволяют использовать это решение в информационных системах любого масштаба.

7 основных достоинств:

- ориентация на применение в крупных современных информационных системах;
- масштабируемость решения;
- высокая производительность решения;
- запатентованный алгоритм анализа трафика statefull inspection;
- широкий перечень дополнительных возможностей;
- снижение совокупной стоимости владения системой обеспечения информационной безопасности;
- авторизованное обучение и возможность получения международного сертификата.

7 ключевых возможностей:

- защита корпоративных ресурсов от внешних злоумышленников и разграничение доступа внутренних пользователей к ресурсам общих сетей;
- аутентификация внешних и внутренних пользователей для доступа к защищаемым ресурсам корпоративной сети и ресурсам Internet;
- скрытие сетевой топологии защищаемой сети;
- защита от вирусов, враждебного мобильного кода (Java, ActiveX, ShockWave и т.д.), а также фильтрация содержания Internet-трафика;

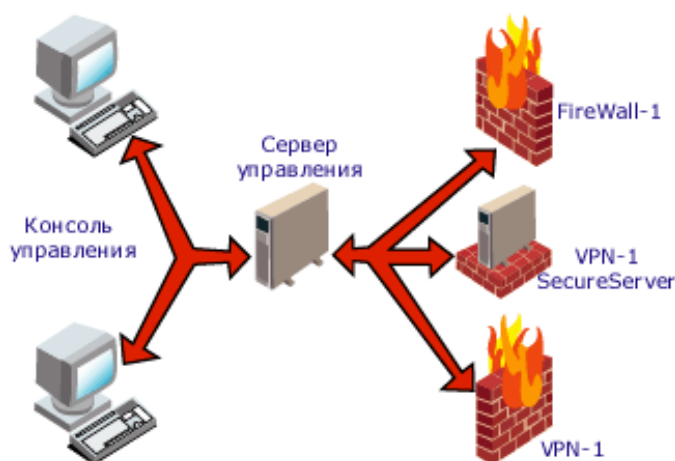
- централизованное управление безопасностью удаленных офисов и филиалов;
- обеспечение высокой доступности и отказоустойчивости;
- балансировка нагрузки между несколькими узлами.

Межсетевой экран **Check Point Firewall-1** является признанным лидером в данной области за счет следующих ключевых возможностей:

- защита корпоративных ресурсов от внешних и внутренних злоумышленников;
- аутентификация внешних и внутренних пользователей для доступа к защищаемым ресурсам корпоративной сети и ресурсам Internet;
- поддержка более 150 сетевых сервисов, протоколов и приложений (включая, H.323, VoIP, RealAudio, Oracle SQL и т.д.);
- скрывание сетевой топологии защищаемой сети;
- защита от вирусов, враждебного мобильного кода (Java, ActiveX, ShockWave и т.д.), а также фильтрация содержания Internet-трафика;
- интеграция с LDAP-сервером для реализации централизованного управления безопасностью всего предприятия;
- централизованное управление безопасностью удаленных офисов и филиалов;
- интеграция с продуктами других фирм ;
- поддержка большого числа платформ ;
- различные уровни доступа по управлению межсетевым экраном;
- обеспечение высокой доступности и отказоустойчивости;
- управление списками контроля доступа маршрутизаторов и серверов удаленного доступа;
- балансировка нагрузки между несколькими узлами;
- генерация большого числа различных отчетов , имеющих как графическое, так и текстовое представление.

Межсетевой экран **Check Point NG** использует трехуровневую архитектуру и состоит из следующих компонентов:

- **VPN-1 (VPN-1 Pro) Gateway** реализует все функции по разграничению доступа, регистрации событий, генерации сигналов тревоги и т.д.
- **SmartCenter (SmartCenter Pro)** управляет всеми подключенными к нему модулями Gateway и другими компонентами, входящими в семейство решений компании CheckPoint.
- **Консоль управления (GUI)** реализует графический интерфейс, облегчающий управление всеми модулями, подключенными к SmartCenter.



Архитектура Check Point NG

5. АНТИВИРУСЫ

- 5.1. Dr.Web
- 5.2. NOD32
- 5.3. Антивирус Касперского

Антивирусные решения. Мы предлагаем следующие антивирусы:

5.1. Dr.Web - Антивирус Dr.Web для Windows – компактный и быстрый антивирус для персональных компьютеров. Обеспечивает многоуровневую защиту системной памяти, файловой системы и всех сменных носителей от всех типов вирусов, троянских программ, шпионского и рекламного ПО, платных программ дозвона, хакерских утилит и программ-шутки. Компоненты Dr.Web позволяют в реальном времени обнаружить и пресечь попытки проникновения на Ваш компьютер вредоносных программ из любых внешних источников.

Подробнее о предлагаемых версиях.

5.2. NOD32 - Антивирус NOD32 - Эффективный способ обеспечения безопасности. Антивирусная система Eset NOD32 позволяет обеспечить сохранность информации и данных от проникновения вредоносных программ через Интернет и электронную почту, и защитить эти и другие данные от всех типов как известных, так и новых угроз. Обнаружение неизвестных угроз обеспечивает собственная технология ThreatSense™. Эта технология - сложная, сбалансированная система продвинутой эвристики и сигнатурного анализа. Ее использование позволяет обеспечить высокий уровень обнаружения, не снижая при этом скорости работы используемой системы.

Подробнее о предлагаемых версиях.

5.3. Антивирус Касперского. "Лаборатория Касперского" - самый известный в России производитель систем защиты от вирусов, спама и хакерских атак. Мы входим в десятку ведущих мировых разработчиков программного обеспечения для защиты информации от интернет-угроз.

"Лаборатория Касперского" - это международная группа компаний с центральным офисом в Москве и представительствами в Великобритании, Германии, Франции, США, Японии, Южной Корее, Китае, Нидерландах, Польше и Румынии. Наша партнерская сеть объединяет свыше 500 компаний более чем в 60 странах мира. "Лаборатория Касперского" - это около 600 высококвалифицированных специалистов.

Подробнее о предлагаемых версиях.

6. СЕТЕВОЙ СКАНЕР УЯЗВИМОСТЕЙ

О компании Positive Technologies www.ptsecurity.ru. Эта компания одна из ведущих российских компаний в области информационной безопасности. Основные направления деятельности компании

- разработка систем комплексного мониторинга информационной безопасности (**XSpider**, **MaxPatrol**);

- предоставление консалтинговых и сервисных услуг в области информационной безопасности;

- развитие специализированного портала Securitylab.ru.

Positive Techno-logies - это команда высококвалифицированных разработчиков, консультантов и экспертов, которые обладают большим практическим опытом, являются членами международных организаций и активно участвуют в развитии отрасли.

Вся информация по продукту **XSpider** находится по адресу <http://www.ptsecurity.ru/xs7.asp> и <http://www.ptsecurity.ru/xs77.asp>.

Информация о **MaxPatrol**:

Система комплексного мониторинга информационной безопасности **MaxPatrol**, разработанная компанией **Positive Technologies**, позволяет получать объективную оценку состояния защищенности, как всей информационной системы, так и отдельных подразделений, узлов и приложений. Механизмы тестирования на проникновение (Pentest), системных проверок (Audit) и контроля соответствия стандартам (Compliance) в сочетании с поддержкой анализа различных операционных систем, СУБД и Web-приложений позволяют **MaxPatrol** обеспечивать непрерывный технический аудит безопасности на всех уровнях информационной системы.

Подробная информация о **MaxPatrol** публикуется на нашем сайте по адресу <http://www.ptsecurity.ru/maxpatrol.asp> .

7. УСТРОЙСТВА ГАРАНТИРОВАННОГО УНИЧТОЖЕНИЯ ИНФОРМАЦИИ НА МАГНИТНЫХ НОСИТЕЛЯХ

- 7.1. Цунами
- 7.2. Системы 2С
- 7.3. Системы СТЕК
 - 7.3.1. Стек - НС1в
 - 7.3.2. Стек - НС2х
 - 7.3.3. Стек - НС2.2км

7.1. "ЦУНАМИ"

Предназначен для защиты информации, расположенной на жестких дисках сервера в автоматическом режиме и ее экстренное уничтожение при попытке несанкционированного доступа (НСД).

Принцип работы. Конструктивно элементы комплекса скрытно монтируются в стандартные компьютерные корпуса, чем обеспечивается высокая степень маскировки и отсутствие явных признаков защиты информационных носителей. При помощи многочисленных датчиков комплекс анализирует внешнюю обстановку и самостоятельно принимает решение: уничтожить информацию или известить пользователя о произошедшем событии (например, отключение электропитания). При нарушении условий охраны производится экстренное уничтожение информации не зависимо от того, происходила работа с ней в момент стирания или нет.

Экстренное уничтожение информации происходит:

- автоматически, *при попытке хищения* (изъятия, выноса) компьютера;
- автоматически, *при попытке вскрытия компьютера* с целью съема накопителей информации;
- автоматически, *через 3 (6, 12, 24) часов после отключения внешнего электропитания;*
- дистанционно *пользователем в любой момент времени.*

Устройство и комплектация. Комплекс может находиться в двух режимах: режим ожидания (РО) и режим охраны (Р1). В режиме РО происходит тестирование всех основных узлов, блоков и датчиков.

В режиме РО происходит тестирование всех основных узлов, блоков и датчиков. Осуществляется свободный доступ к магнитным носителям. В режиме Р1 автоматически происходит уничтожение при попытке НСД или пользователем в любой момент времени:

- нажатием кнопки на корпусе;
- нажатием удаленной кнопки (длина шлейфа до 1000 метров);
- по радиоканалу (дальность до 100 метров);
- по GSM каналу (с сотового телефона набором кода в тональном режиме);
- набором кода на кодовой панели.

Снятие\постановка в режим охраны может осуществляться при помощи электронного ключа ТМ, бесконтактной электронной Proximity карты, сотового телефона или кодовой панели.

Возможно исполнение в корпусах ATX и Rack-Mount 19". НЖМД могут размещаться в съемных шасси Mobile Rack для их оперативной замены.

"ЦУНАМИ" позволяет организовать многоуровневую защиту - контроль нескольких рубежей (например, проникновение в серверное помещение, затем вынос - вскрытие компьютера и т.д.). При этом возможна организация не только контроля, но и доступа в помещение (например, управление замком, выход на общую систему сигнализации...).

Обязательным компонентом комплекса является подсистема энергонезависимого ведения протокола работы с привязкой событий к реальному времени. Данный протокол может быть получен при подключении к комплексу стандартного компьютера (используется СОМ-порт и дополнительное программное обеспечение).

"ЦУНАМИ", являясь законченным автономным решением, все же должен рассматриваться как составная часть комплексной системы безопасности в организации, с обязательной организацией резервного копирования информации, ограничения доступа к охраняемым ресурсам и других методов повышения безопасности.

Дополнительные возможности. За счет модульности, на основе базовых решений можно строить системы защиты самого сложного уровня под практически любые требования пользователя. Здесь будут перечислены основные функциональные решения:

Каналы управления (постановка и снятие с охраны)

Электронный ключ. Представляет собой "таблетку" - идентификатор фирмы Dallas Semiconductor DS-1990. Позволяет однократным поднесением ключа к считывателю производить переключение режима. Таблетка, имея небольшой вес и размеры, высокую надежность и уникальный номер (прошиваемый на заводе, на этапе изготовления) является оптимальным недорогим решением метода "КЛЮЧА".

Proximity - бесконтактная электронная карта. Позволяет скрыто устанавливать считыватель карт, не выдавая само его существование и положение. Карты-идентификаторы уникальны, при высокой надежности, хотя и не самой низкой цене, являются наиболее оптимальным решением метода "КЛЮЧА". Переключение режима производится однократным поднесением ключа-карты на расстояние 3-5 см от считывателя.

Кодовая панель. Позволяет производить переключение режимов набором цифрового кода на панели, которая может быть установлена стационарно или быть отключаемой (съёмной, используемой только в момент переключения режима).

Каналы принудительной активации (запуск уничтожения пользователем)

Проводная кнопка. Нажатие кнопки запускает процесс уничтожения. На кнопке имеется светодиодный индикатор целостности линии (связи с комплексом); Удаленность от комплекса - до 100м.

Управляемая проводная кнопка. Нажатие кнопки запускает процесс уничтожения. На кнопке имеется светодиодная и звуковая индикация режима работы, электропитания, состояния комплекса. Комплексом отслеживается целостность линии до кнопки. Удаленность - до 1000м.

Управление через радиоканал. Запуск уничтожения производится дистанционно, с радиобрелока (аналог автомобильного для сигнализации). Дальность действия - от 40 до 100 м в прямой видимости (наличие помех на пути брелок-комплекс может снизить это расстояние).

Датчики контроля ситуации:

- защита корпуса компьютера от вскрытия;
- защита компьютера от выноса (перемещения);
- защита двери серверного помещения;
- контроль движения в помещении;
- сигнал от внешней системы сигнализации... и т.д.

Дистанционный мониторинг и управление

- ПО для мониторинга и управления комплексом по протоколу TCP-IP (Интернет, локальные сети);

- GSM-канал. Позволяет дистанционно получать SMS-сообщения по сотовой сети о событиях комплекса, производить экстренную активацию комплекса.

Прочее. Комплекс "Цунами" разрабатывался как максимально гибкая система для удовлетворения практически любых требований к охране, предъявляемых в различных сферах деятельности организаций. Поэтому описывать все возможности и модификации нецелесообразно и невозможно. Для каких-то специфических условий возможно исполнение и разработка нового решения.

Изготовление "Цунами"

Изготовление каждого производится только по Техническому Заданию (ТЗ), утверждаемому Заказчиком и представителем производителя. В ТЗ отражаются особенности реализации и функционирования, конечная стоимость и сроки выполнения работ. На основании данного документа производится изготовление и сдача в эксплуатацию оборудования.

8.2. Системы 2С

8.2.1. 2С-994iR - Устройство мгновенного стирания информации с НЖМД.

Назначение. Устройство 2С-994iR предназначено для мгновенного и необратимого стирания информации с накопителя на жестком магнитном диске (НЖМД).

Конструктивно 2С-994iR является комплексом взаимосвязанных модулей, устанавливаемых в стандартный корпус компьютера пользователем. Устройство рассчитано на продолжительный режим работы.

Условия применения. Рабочие условия применения Устройства:

- температура окружающей среды от +10оС до +50 оС ;
- относительная влажность воздуха до 75%;

Комплект поставки

- | | |
|----------------------------------|--------|
| - блок стирания 2С-994 | 1 шт.; |
| - источник автономного питания | 1 шт.; |
| - блок радиоуправления | 1 шт.; |
| - радиобрелок управления | 2 шт.; |
| - кнопка активации | 1 шт.; |
| - кабель внешнего электропитания | 1 шт.; |
| - технический паспорт | 1 шт.; |

Основные технические данные и характеристики. Параметры и характеристики устройства приведены в таблице

Таблица 7.1. - Параметры и характеристики устройства стирания данных на НЖМД - 2С-994iR

Наименование показателей, единицы измерения	Значение
1. Тип	Встраиваемый
2. Количество подключаемых модулей уничтожения 2с-994 , шт.	1
3. Время до полного заряда комплекса после включения, сек, не более	120
4. Электропитание устройства	220±10% В, 50 Гц
5. Потребляемый ток, мА	
в режиме заряда аккумуляторов(отключенном блоке управления)	110
в режиме заряда модуля уничтожения	150
в рабочем режиме	120
6. Дальность действия радиобрелков без препятствий в прямой видимости, метров	До 40
7. Время работы в автономном режиме в случае отключения внешнего питания при полностью заряженных аккумуляторах, часов, не менее	48
8. Время полного заряда аккумуляторов от внешней сети, часов	40
9. Суммарная масса блоков, кг, не более	7
10. Время до повторного включения устройства после стирания, сек, не менее	60
11. Установленный ресурс работы, лет, не менее	2

8.3. Системы СТЕК

8.3.1. Стек – НС1в.

Устройство "Стек – НС1в" предназначено для гарантированного уничтожения информации, записанной на НЖМД с продольным и наклонным типами записи, и соответствует требованиям Приказа МО РФ № 306 от 10.08.02 г. Соответствие подтверждается сертификатом Минобороны России.



Устройство "Стек – НС1в"

Основные особенности Изделия:

- предельно возможная скорость стирания информации (доли секунды);
- способность находиться в состоянии "Готовность" сколь угодно долго без ухудшения характеристик;
- высокая надежность вследствие отсутствия механически движущихся частей;
- стирание информации, записанной на магнитном носителе, происходит без его физического разрушения;
- стирать информацию можно с неисправных носителей;
- конструкция рабочей камеры позволяет стирать информацию с НЖМД в салазках "Горячей замены" наиболее распространенных типов;
- изделие оснащено встроенным измерителем амплитуды стирающего поля;
- параметры стирающего поля и конструкция рабочей камеры позволяют эффективно уничтожать информацию на большом количестве магнитных носителей других типов;
- изделие опционно поддерживает возможность удаленного пуска и мониторинга: амплитуда поля, исправность основных элементов, режим работы (исполнение "под заказ").

Проведенная в испытательной лаборатории фирмы "Анна" экспертиза дала положительные результаты для следующих магнитных носителей информации:

- 1) компакт-кассеты пленочных аудиомagnetофонов всех типов;
- 2) пленки видеомagnetофонов всех типов;
- 3) пленки стримеров;
- 4) дискеты 3,5";
- 5) Zip- и Jaz-диски.

После стирания информации повторное использование магнитных носителей первого, второго, третьего и четвертого типов возможно без ограничений (для дискет достаточно выполнить штатное форматирование). Повторное использование НЖМД, Zip- и Jaz-дисков невозможно без предформатирования с использованием специального оборудования.

Таблица 8.2. - Основные технические характеристики Изделия.

Параметр	Значение
Размеры рабочей камеры: - габаритные - активной части	38x222x118 мм 38x105x118 мм
Импульс стирающего магнитного поля: - напряженность в активной части рабочей камеры - ориентация вектора намагничивания	не менее 495 кА/м перпендикулярно плоскости входного окна
Продолжительность выхода в режим "Готовность"	не более 10 с
Минимальная пауза между повторными запусками процесса стирания	10 сек
Продолжительность стирания информации	не более 0,1 с
Способы инициализации	кнопка "Пуск" на передней панели
Продолжительность работы в режиме "Готовность"	не ограничена
Электропитание изделия	сеть ~220 В / 50 Гц
Ток, потребляемый от сети питания	не более 3 А
Условия эксплуатации: - температура окружающей среды - относительная влажность воздуха	от 5 до 40° С до 70 % при t° = 25° С

Габариты	158x158x330 мм
Масса изделия	не более 5 кг

8.3.2.Стек - НС2х.

Основными особенностями изделий являются:

- возможность долговременной (круглосуточной) эксплуатации НЖМД, находящихся в рабочей камере, т.к. обеспечены теплоотвод и надежное механическое крепление НЖМД, а также защита от случайного срабатывания устройства;
- возможность дистанционного и (или) автоматического пуска;
- возможность обеспечения автономного (бесперебойного) электропитания. НЖМД устанавливается внутрь стирающего модуля и фиксируется винтами на специальных салазках.



Изделия серии “Стек-НС2х” (“Стек-НСА2х”)

Изделия серии “Стек-НС2х” (“Стек-НСА2х”) предназначены для использования в качестве ядра информационных сейфов и обеспечивают быстрое (экстренное) уничтожение информации, записанной в НЖМД, эксплуатируемых в момент стирания.

Обдув НЖМД, помещенных в устройства “Стек” осуществляется встроенными в рабочие камеры вентиляторами.

Внимание! После стирания информации повторное использование НЖМД невозможно без предформатирования с использованием специального оборудования.

Информационные сейфы можно классифицировать по двум признакам:

1	По количеству рабочих камер:	1-о и 2-х камерные устройства
2	По способу питания:	- только сеть ~220 В; - сеть 220 В + гарантированное автономное питание (от 2 до 48 час)

Устройства “Стек-НС2м” и “Стек-НСА2м” предназначены для создания информационных сейфов для одиночных НЖМД и ориентированы на установку внутри системного блока компьютера вместо двух или трех пятидюймовых устройств.

Типовое значение максимальной рабочей температуры НЖМД 55°С.

Модель НС2м имеет только сетевое электропитание.

Модель НСА2м кроме сетевого электропитания имеет встроенный источник автономного питания.

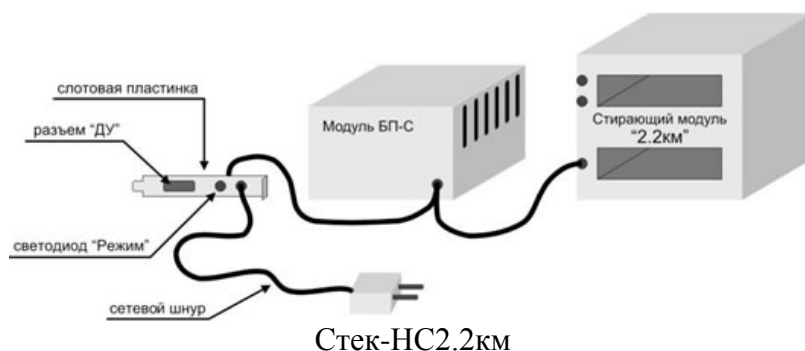


Таблица 8.3. - Основные технические характеристики Стек-НС2м и Стек-НСА2м

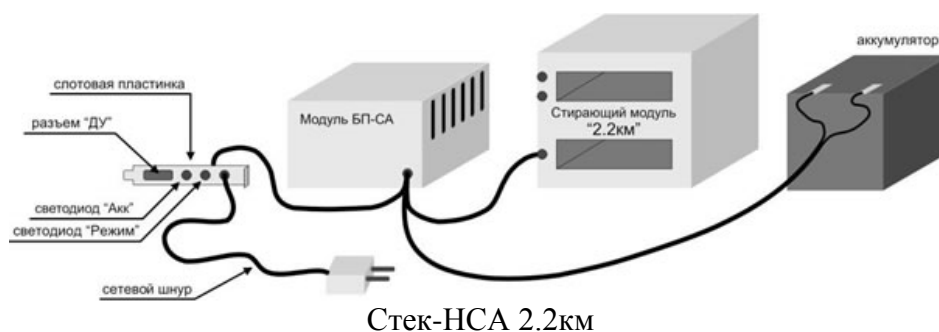
Параметр	Стек-НС2м	Стек-НСА2м	
		при питании от сети ~220В	при автономном питании
Габаритные размеры рабочей камеры	189х110х29 мм (устройство 3,5 дюйма)		
Напряженность импульса стирающего магнитного поля	не менее 400 кА/м		
Длительность импульса стирающего магнитного поля	не более 3 с	не более 3 с	не более 10 с
Продолжительность стирания информации на одном носителе	не более 0,1 сек		
Макс. задержка с момента пуска до окончания стирания	1,5 с	1,5 с	не более 12с (холодн.пуск) не более 3 с (теплый пуск)
Продолжительность работы в режиме “Готовность”	не ограничена	не ограничена	8...16 ч *)
Максимальная тепловая мощность, отводимая от НЖМД	15 Вт, см рис 1.3		
Способ инициализации	внешнее устройство, подключаемое к разъему “ДУ”		
Электропитание Изделия	сеть ~220В / 50 Гц	сеть ~220В / 50 Гц + аккумулятор	
Габаритные размеры	150 х 85 х 230	150 х 85 х 230 мм (стирающий модуль) 150 х 42 х 240 мм (модуль ИБП)	

Примечание. *) Точное значение определяется:

- выбором вида пуска – “холодный” или “теплый”;
- количеством дополнительных нагрузок (контролеры управления).

7.3.3. Стек - НС2.2км.

Устройства для защиты RAID-массивов НЖМД. Устройства “Стек-НС2.2км” и Стек-НСА2.2км предназначены для создания информационных сейфов для RAID-массивов НЖМД и ориентированы на установку внутри системного блока компьютера на места трех пятидюймовых устройств и дополнительного источника электропитания. Использование групповых модулей позволяет добиться существенного снижения затрат на 1 НЖМД.



Устройства этого класса позволяют питать развитые системы дистанционного и (или) автоматического управления, а так же использовать для автономного электропитания аккумуляторы большой емкости.

Внутри каждого стирающего модуля может быть установлено по 2 НЖМД.

Модульная конструкция позволяет создавать системы и на большее количество НЖМД в RAID-массиве.

Основные технические характеристики устройства Стек-НС2.2км

Параметр	Значен
Количество рабочих камер	2
Габаритные размеры рабочей камеры	145х105х28 мм (устройство 3,5 дюйма)
Напряженность импульса стирающего магнитного поля	не менее 400 кА/м
Максимальная продолжи-тельность выхода в режим “Готовность” после подачи питания	не более 15 с
Длительность импульса стирающего магнитного поля	0,01 сек

Максимальная задержка с момента пуска до окончания стирания	$T = 1,5c \times (\text{число НЖМД})$
Продолжительность автономной работы в режиме "Готовность"	не ограничена
Максимальная тепловая мощность, отводимая от каждого НЖМД.	15 Вт, см рис 1.5 *)
Способ инициализации	внешнее устройство, подключаемое к разъему "ДУ"
Электропитание Изделия	сеть ~220В / 50 Гц
Габаритные размеры	150 x 130 x 230 мм (стирающий модуль)
Вес	7,0 кг

Примечание. *) Вентиляторы для отвода тепла питаются от источника компьютера (+12В).

9. Оборудование для защиты помещений от утечки информации

9.1. Аппаратура защиты информации от акустической защиты

9.1.1. Генератор акустического шума ЛГШ-301.

9.1.2. Зашумляющая акустическая система ХАОС.

9.1.3. Модели 1М аппаратуры «Соната АВ».

9.1.4. Модели ДУ2mini и ДУ-K2.

9.1.5. Соната - РК1

9.1.6. Соната - PC1 ,PC2

9.1.7. Соната - P2

9.2. Защита слаботочных коммуникаций

9.2.1. Устройство защиты Корунд.

9.2.2. Устройства защиты МП.

9.1.1. Генератор акустического шума ЛГШ-301

ЛГШ-301 предназначен для защиты речевой информации от перехвата по прямому акустическому, виброакустическому и оптикоакустическому каналам. Он используется в условиях замкнутого пространства с питанием от сети переменного тока 220 В и защищает пространство объемом до 50 м³. При работе в помещении большего объема, необходимо устанавливать несколько генераторов. Принцип действия основан на генерации "белого шума" в акустическом диапазоне частот и, как следствие, повышении отношения акустическая помеха/речевой сигнал. Монтировать генераторы рекомендуется в непосредственной близости к местам возможного размещения системы перехвата, таким как: оконные и дверные проемы, стены, потолки и полы помещений, вентиляционные каналы и воздуховоды, трубы систем центрального отопления и водоснабжения, стекла и тонкие перегородки. ЛГШ-301 чаще всего используется в комплексе с другими средствами защиты информации.



Генератор акустического шума ЛГШ-301

В прошлом при разработке и внедрении комплексных систем защиты информации от утечки по техническим каналам для зашумления перечисленных "слабых" мест использовались генераторы акустического шума других фирм-производителей, например, - Смерш Техникс. Эти генераторы (последняя версия WNG-023) при включении устанавливаются в среднее положение уровня громкости шума, которое затем можно регулировать. Это очень удобно для "карманного" использования.

Однако устройства подобного типа не предназначены для монтажа, подразумевающего автономную работу. Это привело специалистов ЛабППШ к идее создания ЛГШ-301 специально для использования в стационарных условиях.

Комплектность поставки

Наименование

Количество

Основной блок

1

Блок питания	1
Отвертка*	1
Руководство по эксплуатации	1
Упаковка	1

* - устройство комплектуется отверткой для регулирования уровня громкости

Технические характеристики.

Характеристика	Значение
Основной блок	
Габаритные размеры	66×66×20 мм
Масса	100 г
Рабочее напряжение	5 В (±1%)
Параметры входного акустического сигнала основной диапазон частот (речевой диапазон)	300–3400 Гц
Сопротивление излучающей головки	8 Ом
Блок питания	
Габаритные размеры	70×47×86 мм
Масса	120 г
Рабочее напряжение	220 В (±10%), 50 Гц
Выходная мощность	1.5 Вт
Выходное напряжение	5 В (±1%)

9.1.2. Зашумляющая акустическая система ХАОС.

Зашумляющая акустическая система ХАОС предназначена для предотвращения несанкционированного перехвата акустической (речевой) информации средствами акустического контроля: радио микрофонами, проводными микрофонами, стетоскопами, любыми типами диктофонов, в т.ч. встроенными в сотовые телефоны, направленными микрофонами и т.д. Также она обеспечивает защиту от утечки через технические средства, обладающие "микрофонным эффектом", или к которым применимо использование метода "высокочастотного навязывания"

Система ХАОС является универсальным прибором и может использоваться как в стационарных, так и в мобильных (неподготовленных) условиях, и рассчитана на длительный срок непрерывной эксплуатации.

Переговоры осуществляются с помощью наушников с шумопоглощающими гарнитурами и специальных микрофонов. Речевые сигналы, поступающие с микрофонов, подвергаются обработке для отсева шумовой составляющей. Имеется возможность индивидуальной регулировки громкости и отключения микрофонов. Речь говорящего абонента, перехватываемая средствами контроля, представляет собой смесь "речевой помехи", создаваемого прибором и речи абонента. Выделение последней становится практически нерешаемой задачей.



Зашумляющая акустическая система ХАОС

Технические характеристики.

тип помехи	речевой хор
количество защищаемых абонентов	4
выходная мощность акустической системы	5 Вт
напряжение питания	220 В/ 50 Гц или 12 В (от бортовой сети автомобиля)

9.1.3. Модели 1М аппаратуры «Соната АВ»

Системы акустической и виброакустической защиты семейства "Соната-АВ" предназначены для защиты речевой информации, циркулирующей в выделенных (защищаемых) помещениях, от утечки по акустическим и виброакустическим каналам.



Аппаратура «Соната АВ».



Виброизлучатели ВИ-45 и ПИ-45

Система виброакустической и акустической защиты "Соната-АВ" (модель 1М), является техническим средством защиты речевой информации от утечки по акустическому и виброакустическому каналам путем формирования шумового сигнала речевого диапазона частот в соответствии с требованиями "Сборника нормативно-методических документов по противодействию акустической речевой разведке" (НМД АРР-2000). Система не образует каналов утечки информации за счет акустоэлектрических преобразований, может устанавливаться в выделенных помещениях до 1 категории включительно и соответствует требованиям технических условий АРЕМ.468781.003 ТУ. Соответствие подтверждается сертификатом ФСТЭК России.

В состав аппаратуры "Соната-АВ" (модели 1М) входят следующие базовые элементы:

Базовый элемент	Тип базового элемента	
	Модель 1М	Модель 2М
“Тяжелый” виброизлучатель	ВИ-45	
“Легкий” виброизлучатель (“пьезоизлучатель”)	ПИ-45	
Аудиоизлучатель	АИ-65	
Генераторный блок	«Соната АВ модель 1М»	«Соната-АВ модель 2М»

Основными отличиями генераторного блока модели 2М от 1М являются:

- более высокая нагрузочная способность;
- возможность корректировки спектра шума, что позволяет в ряде случаев снизить интегральный уровень шума (а, следовательно – мешающее действие системы) без снижения стойкости защиты.

Основные технические характеристики генераторных блоков

Параметр	Значение	
	мод. 1М	мод. 2М
Количество независимых каналов ¹⁾	2	
Максимальное ²⁾ количество одновременно подключаемых:		
· виброизлучателей ВИ-45	20 (10+10)	40 (20+20)
· аудиоизлучателей АИ-65	16 (8+8)	20 (10+10)
· пьезоизлучателей ПИ-45	16 (8+8)	16 (8+8)
Полоса частот генерируемого электрического сигнала	175 - 5600 Гц	
Превышение вибрационного и акустического шума над уровнем речевого сигнала в канале утечки информации	не менее 10 дБ	
Наличие входа ДУ (интерфейс)	есть, (НР контакт)	
Электропитание изделия	Сеть ~220 В / 50 Гц	
Габариты блока	200x70x245 мм	
Вес блока	2,9 кг	

Условия эксплуатации:	
- температура окружающей среды	С°от 5 до 40
- относительная влажность воздуха	° = 25°до 70 % при t C
Продолжительность непрерывной работы Изделия, не менее	24 час

Примечания:

1) “Независимость” заключается,

- в наличии отдельного генератора в каждом канале устройства, что позволяет увеличить стойкость системы виброакустической защиты за счет использования на одном и том же элементе конструкции помещения излучателей подключенных к разным каналам генератора;
- в возможности изменения выходного напряжения шумового сигнала независимо на каждом канале;
- в возможности установки вида нагрузки отдельно для каждого канала.

Дистанционное включение/отключение каналов осуществляется одновременно.

2) Значение указано на наихудший случай – когда все без исключения излучатели, подключенные к генераторному блоку, должны обеспечивать максимально возможный интегральный уровень.

Основные технические параметры и характеристики излучателей:

Параметр	ПИ-45	ВИ-45	АИ-65
Полоса воспроизводимых частот	175 – 5 600 Гц *)		
Размах напряжения входного сигнала	не более 30 В	не более 100 В	не более 1 В
Эквивалентное сопротивление	300 Ом	500 Ом	8 Ом
Эквивалентная емкость	20 нФ	6 нФ	-
Продолжительность непрерывной работы Изделия	не ограничена		
Габариты Изделия	D= 50 мм H= 5 мм	D= 45мм H= 40 мм	40x70x125 мм
Вес Изделия	0,01 кг	0,3 кг	0,3 кг
Условия эксплуатации:			
- температура окружающей среды	С°от 5 до 40		
- относительная влажность воздуха	° = 25°до 70 % при t C		

*) Параметр гарантирован только при выполнении следующих условий:

- излучатели АИ-65, ВИ-45 и ПИ-45 подключаются к генератору “Соната-АВ” модели 1М и 2М производства ЗАО “Анна”;
- к одному выходу генератора подключаются излучатели только одного типа;
- подключение только параллельное;
- тип нагрузки и тип выхода генератора находятся в соответствии.

Виброизлучатель ВИ-45 является специализированным электроакустическим преобразователем повышенной мощности и предназначен для возбуждения шумовых вибраций в массивных конструкциях защищаемого помещения, обеспечивая при этом приемлемый уровень мешающего акустического шума. Конструкция и размеры виброизлучателей и элементов их крепления оптимизированы для их установки:

- на ограждающих конструкциях помещения (стены, потолок, пол, двери);
- на массивных окнах;
- на трубах систем тепло-, водо- и газоснабжения.

Виброизлучатель ПИ-45 является специализированным электроакустическим преобразователем малой мощности и предназначен для возбуждения шумовых вибраций в остеклении окон (дверей, офисных перегородок и т.п.).

Аудиоизлучатель АИ-65 является специализированным электроакустическим преобразователем и предназначен для возбуждения акустического шума. Конструкция и размеры аудиоизлучателя и элементов их крепления оптимизированы для его установки:

- в надпотолочном пространстве;
- в вентиляционных каналах;
- дверных тамбурах.

В случае, если по каким-либо соображениям указанные условия невыполнимы, выбор схемы подключения необходимо осуществлять, принимая во внимание следующее:

1) Опасность вывода генераторных блоков из строя путем перегрузки каналов отсутствует.

2) При увеличении количества подключаемых к одному каналу излучателей сверх нормы, основной проблемой может стать дефицит интегрального уровня шума (прежде всего для АИ-65), либо высокочастотных составляющих спектра шума (для ВИ-45 и ПИ-45). Это также является нарушением условий сертификации, а также руководства по эксплуатации, что может привести к отказу системы.

3) При объединении в одну группу излучателей различных типов, основной проблемой может стать одновременное выполнение требований к интегральному уровню шума у излучателей разного типа (либо избыток у одних, либо дефицит у других).

9.1.4. Модели ДУ2mini и ДУ-К2.



ДУ2mini



ДУ-К2

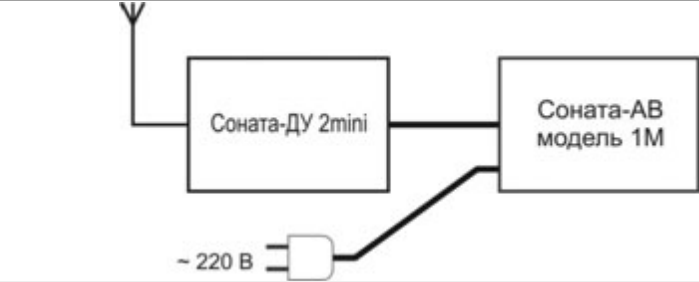
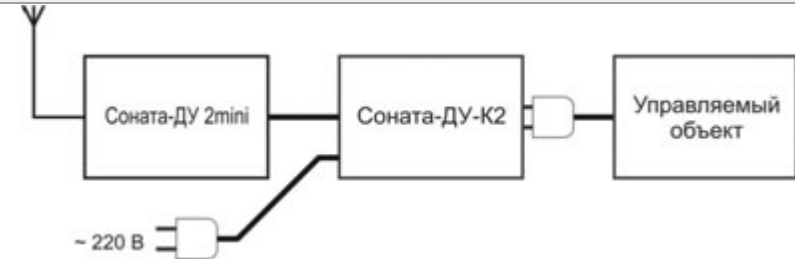
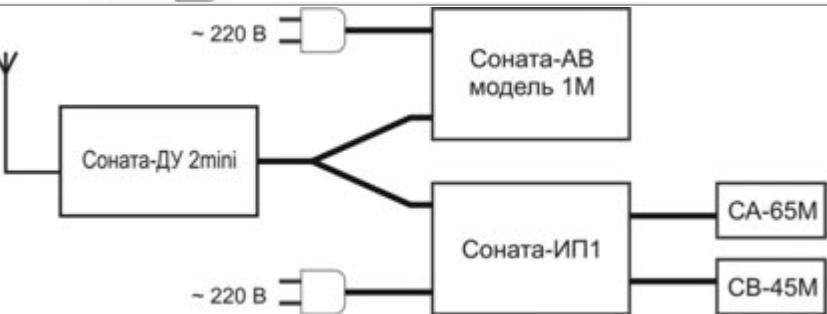
Основные технические характеристики Изделия:

Параметр	Значение	
	Модель ДУ2mini	Модель ДУ-К2
Количество независимых каналов включения/отключения	2	2
Количество групп контактов “на переключение” в каждом канале	1	1 (220 В)
Нагрузочная способность одной коммутируемой цепи	$I_{\text{н}} = \text{до } 50 \text{ мА}$, $I_{\text{с}} = \text{до } 100 \text{ мА}$, $U_{\text{ком}} = 5 \dots 30 \text{ В}$	Канал 1: 0...100 Вт Канал 2: 20...500 Вт
Выходное напряжение на каждом сетевом канале	нет	~220 В ($\pm 10\%$), 50 Гц ($\pm 5\%$)
Варианты управления	радиобрелок	вход ДУ (DB-9F)
Дальность действия радиобрелка	не менее 10 м	нет
Электропитание изделия: Моноблок	12 В	Сеть ~220 В ($\pm 10\%$), 50 Гц ($\pm 5\%$)
Радиобрелок	батарея типа MN21 (A23-3LR50)	нет
Продолжительность непрерывной работы	24 ч	
Габариты	90x30x105 мм	51x51x180 мм
Срок службы батареи радиобрелка (10 включений в день)	не менее 12 месяцев	

Применение этих моделей позволяет значительно сократить как сроки, так и стоимость проектирования и монтажа сложных комплексов защиты речевой информации, а также существенно повысить удобство эксплуатации систем, в состав которых они включаются.

Типовые решения на базе моделей ДУ2mini и ДУ-К2.

Выпускаемая ЗАО “Анна” аппаратура серии “Соната” разработана с учетом возможности ее гибкого и малоизбыточного комплексования. Представление о возможностях по комплексованию дают варианты типовых решений наиболее часто встречающихся задач, представленные в таблице.

<p><u>“Миникомплекс активной виброакустической защиты”:</u></p> <ul style="list-style-type: none"> - Предельная простота стыковки элементов. - Существенное упрощение монтажа (беспроводное включение). 	
<p><u>“Система дистанционного включения нештатного оборудования”:</u></p> <ul style="list-style-type: none"> - Возможно беспроводное управление оборудованием, не имеющим спец. входов; - Простота создания комплекса 	
<p><u>“Система комплексной защиты помещения”:</u></p> <ul style="list-style-type: none"> - Возможность независимого управления 2 типами оборудования; - Большой спектр решений, реализуемых “без паяльника”. 	

9.1.5. Устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН “Соната-РК1”.

Устройство комбинированной защиты “Соната-РК1” предназначено для защиты информации, обрабатываемой основными техническими средствами и системами до 1 категории включительно, от утечки за счет ПЭМИН путем постановки маскирующих помех в линиях электропитания и заземления, а также путем пространственного зашумления и частичного поглощения информативных сигналов, распространяющихся по линиям электропитания и заземления.



Устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН “Соната-РК1”.

Устройство комбинированной защиты объектов информатизации от утечки информации по техническим каналам "Соната-РК1" соответствует требованиям "Норм эффективности защиты АСУ и ЭВМ от утечки информации за счет побочных электромагнитных излучений и наводок" и технических условий ЮДИН.665820.002 ТУ. Устройство может использоваться для защиты объектов ЭВТ, а также устанавливаться в выделенных помещениях до 1 категории включительно без принятия дополнительных мер защиты акустической речевой информации. Соответствие подтверждается сертификатом ФСТЭК России.

Особенности конструкции устройства "Соната-РК1" позволяют получать эффективное и недорогое решение задачи комплексной защиты ("ПЭМИ + наводки на ВТСС и их линии + наводки на линии электропитания и заземления") объекта вычислительной техники состоящего из одиночного средства вычислительной техники в ситуациях, когда остро стоит проблема помех, создаваемых генераторами маскирующего шума.

Устройство "Соната-РК1" является комбинацией фильтра поглощающего типа, генераторов шумового тока с корректировкой спектра и регулировкой интегрального уровня и элементов антенной системы.

При этом:

1) кривая ослабления фильтра и частотный спектр мощности маскирующей помехи взаимно дополняют друг друга ;

2) возможность корректировки спектра создает условия для снижения интегрального уровня маскирующей помехи на основе "прицеливания" по частоте;

3) частью антенной системы является включаемое через изделие, как через сетевой удлинитель, защищаемое техническое средство. Такое решение создает условия для снижения интегрального уровня маскирующей помехи на основе "автоматического" прицеливания по каналам распространения ПЭМИ.

Кроме того, устройство может быть использовано как объектовый генератор шумового ЭМИ. Для этого в его сетевой выход необходимо включить более ни к чему не подключенный сетевой шнур от компьютера и вытянуть всю конструкцию в вертикальную прямую линию . Располагать генераторы целесообразно вдоль границы КЗ.

Если розетку сети 220В выбрать на границе КЗ (по аналогии с изделием "Соната-РС1"), то устройство будет работать и в качестве объектового генератора шума по сети электропитания и линиям заземления.

Основные технические характеристики:

Параметр	Значение
Диапазон генерируемых частот	0,01...1000 МГц
Спектральная плотность мощности радиоизлучения, дБ относительно 1 мкВ/м/ОкГц, на расстоянии 1 м не менее	
- в полосе 0,1 ... 0,3 МГц	60
- в полосе 0,3 ... 30 МГц	50
- в полосе 30 ... 300 МГц	45
- в полосе 300 ... 1000 МГц	30
Спектральная плотность напряжения шумов на нагрузке 3 Ом, дБ относительно 1 мкВ/ОкГц, не менее:	
- в полосе 0,01 ... 0,15 МГц	35
- в полосе 0,15 ... 30 МГц	50
- в полосе 30 МГц ... 1000 МГц	35
Диапазон плавного регулирования уровня шума на выходе устройства, не менее, дБ:	
- в полосе «А» (ориентировочно 0,01 ... 1,5 МГц)	15
- в полосе «В» (ориентировочно 0,1 ... 30 МГц)	10
- в полосе «С» (ориентировочно 30 ... 1000 МГц)	10
Коэффициент направленного действия в горизонтальной плоскости, не более	4
Коэффициент качества шума, не менее	0,8

Коэффициент межспектральных корреляционных связей шума, не более	2
Максимальная мощность нагрузки, подключаемой через изделие.	1 кВт
Электропитание изделия	сеть ~220В / 50 Гц
Габаритные размеры	65 x 80 x 265 мм
Продолжительность непрерывной работы, не менее	24 ч

9.1.5. Устройства для защиты линий электропитания и заземления от утечки информации “Соната-РС1” и “Соната-РС2”.

Устройства для защиты линий электропитания, заземления от утечки информации “Соната-РС1” и “Соната-РС2” предназначены для активной защиты объектов ВТ (объектов вычислительной техники) от утечки информации за счет наводок на линии электропитания и заземления.



“Соната-РС1” и “Соната-РС2”

Генератор шума по сети электропитания и линиям заземления “Соната-РС1” является техническим средством защиты информации, обрабатываемой на объектах вычислительной техники 1, 2 и 3-й категорий от утечки за счет наводок информативных сигналов в линии электропитания и заземления, соответствует требованиям документов: “Сборник норм защиты информации за счет побочных электромагнитных излучений и наводок”, “Средства активной защиты объектов ЭВТ от утечки информации по побочным электромагнитным излучениям и наводкам. Основные технические требования.” Соответствие подтверждается сертификатом ФСТЭК России.

Устройство защиты объектов информатизации от утечки информации по сети электропитания и линиям заземления “Соната-РС2” является техническим средством защиты информации, обрабатываемой на объектах вычислительной техники 1, 2 и 3-й категорий от утечки за счет наводок по цепям электропитания и заземления путем постановки помех в диапазоне частот 0,1...2000 МГц и соответствует требованиям технических условий ЮДИН.665820.004 ТУ. Устройство может использоваться в выделенных помещениях до 1 категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. Соответствие подтверждается сертификатом ФСТЭК России.

Особенности конструкции устройств позволяют получать эффективные и недорогие решения при оборудовании объекта вычислительной техники с большим количеством средств вычислительной техники (СВТ). Вариант установки Изделий на объекте ВТ с одним вводом линии 220 В см. рис. 2.1, с двумя вводами рис. 2.2.

Изделия рассчитаны на подключение к 3-проводной сети энергоснабжения («Фаза», «Ноль» и «Защитное заземление») и обеспечивают формирование несинфазных токов и синфазных и паразитных составляющих шумового напряжения во всех проводниках. При нарушении схемы подключения наличие всех составляющих, а так же значение интегрального уровня шума может не обеспечиваться.

Основные технические характеристики Изделий:

Параметр	Соната-PC1	Соната-PC2
Коэффициент качества шума	не менее 0,8	
Коэффициент межспектральных корреляционных связей шума	не более 3	
Спектральная плотность напряжения шумов на нагрузке 3 Ом (Дб относительно к 1 мкВ/ $\sqrt{\text{кГц}}$) в диапазонах частот : 0,01 – 0,15 МГц 0,15 – 30 МГц 30 – 1000 МГц 1000 – 2000 МГц	не менее 35 не менее 50 не менее 35 -	не менее 35 не менее 50 не менее 35 не менее 35
Модуль минимального сопротивление нагрузки	3 Ом	
Глубина регулировки интегрального уровня шума на выходе устройства	не менее 10 дБ	
Индикация системы контроля интегрального уровня шумового напряжения	светодиодная	светодиодная, звуковая
Наличие системы контроля правильности подключения	нет	да
Продолжительность непрерывной работы	не менее 24 час	
Время выхода Изделия в рабочий режим после включения	не более 5 с	
Наличие ДУ (интерфейс)	есть (нормально разомкнутый контакт)	
Электропитание Изделия	~220 В / 50 Гц	
Габаритные размеры	140 x 70 x 170 мм	

В устройстве имеется встроенный источник постоянного тока для электропитания внешних устройств с параметрами: напряжение 10 - 15 В, при токе в нагрузке до 30 мА.

9.1.6. Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН "Соната-Р2".



Устройство защиты объектов информатизации от утечки информации по техническим каналам "Соната-Р2", предназначено для защиты объектов ВТ (вычислительной техники) до 1-й категории включительно от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии вспомогательных технических средств.

Устройство "Соната-Р2" является техническим средством защиты информации, от утечки информации за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума и соответствует требованиям "Норм защиты информации, обрабатываемой средствами вычислительной техники и в автоматизированных системах, от утечки за счет побочных электромагнитных излучений и наводок" и технических условий ЮДИН.665820.003 ТУ. Устройство может устанавливаться в выделенных помещениях до 1 категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации. Соответствие подтверждается сертификатом ФСТЭК России

Основные технические характеристики:

Параметр	Значение
Спектральная плотность электрической составляющей электромагнитного поля Еш шума (ЭМПШ) на расстоянии 1 метр от излучателя, дБ(мкВ/м/√кГц), не менее	
- 1 ... 10 МГц	40
- 10 ... 100 МГц	30
- 100 ... 2000 МГц	25
Спектральная плотность магнитной составляющей электромагнитного поля рНш шума (ЭМПШ) на расстоянии 1 метр от излучателя, дБ(мкВ/м/√кГц), не менее	
- 1 ... 10 МГц	20
- 10 ... 30 МГц	30
Спектральная плотность напряжения шума, наводимого САЗ в цепях электропитания и заземления дБ(мкВ/√кГц), не менее:	
- 0,1 ... 10 МГц	30
- 10 ... 100 МГц	20
- 100 ... 1000 МГц	10
Коэффициент качества шума, не менее	0,8
Коэффициент межспектральных корреляционных связей шума, не более	1,1
Коэффициент направленного действия антенной системы устройства, не более	4
Коэффициент поляризации антенной системы устройства, не более	3
Глубина регулирования интегрального уровня шума на выходе устройства в диапазоне, не менее	10 дБ
Контроль работоспособности	Светодиодная и звуковая индикация нормального режима работы
Электропитание изделия	сеть 220 В / 50 Гц
Мощность потребляемая от сети, не более	10 Вт
Габаритные размеры	D = 65, H = 325
Максимальная продолжительность непрерывной работы, не менее	24 час

9.1.7. Устройство защиты Корунд.

Устройство защиты Корунд предназначено для исключения утечки информации через абонентскую линию аналоговых АТС, является ПСЗ и представляет собой фильтр. Устройство обеспечивает затухание сигналов малого уровня от ТА в сторону абонентской линии.



Устройство защиты Корунд

Технические характеристики:

- защита аналоговых АТС;
- защита от микрофонного эффекта;
- принцип работы - ограничение малых сигналов;
- затухание сигнала: со стороны "ТА" в сторону "линия" на частоте 1000 Гц при $U_{\text{сиг}}$ меньше 50 мВ - более 60 дБ;
- затухание речевых сигналов менее 2 дБ;
- устройство пассивное питание не требует;
- устанавливается внутри евророзеток и безобрывных розеток типа РТШ-4;
- габариты - 40x13x10 мм;
- изделие сертифицировано Гостехкомиссией России

9.1.8. Устройства защиты МП.

Устройства защиты МП-1А и МП-1Ц предназначены для исключения утечки информации через абонентскую линию аналоговых и цифровых АТС соответственно, в режиме ожидания вызова. В них одновременно используются как пассивные средства защиты (ПСЗ), так и активные средства защиты (АСЗ). Устройства содержат генератор шума, нелинейные цепи и узел подавления сигналов малого уровня, с помощью которых обеспечивается введение шумового сигнала в абонентскую линию, затухание сигнала малого уровня от ТА в сторону абонентской линии и защита информации от утечки при активных методах воздействия в режиме ожидания вызова. Они отличаются малыми габаритами и низкой потребляемой мощностью по сравнению с ближайшими прототипами типа Гранит-8,11,12., это позволяет разместить их внутри телефонных розеток. Эксплуатационные расходы по изделию МП-1А не требуются, а по МП-1Ц сводятся к периодическому аудиоконтролю наличия шума в абонентской линии



Устройства защиты МП-1А и МП-1Ц

Технические характеристики изделий МП-1А и МП-1Ц.

Модель	Назначение	Защита от микрофонного эффекта	Полоса частот шумового сигнала	Ток потребления	Вносимое затухание	Габариты без корпуса	Наработка на отказ
МП-1А	Защита аналоговых ТА	Есть	0.02-30 кГц	не менее 0.42 А	не менее 68 дБ	не более (32x15x13) мм	не менее 100000 ч.
МП-1Ц	Защита цифровых ТА	Есть	0.02-300 кГц	не менее 0.42 А	не менее 43 дБ	не более (32x15x13) мм	не менее 100000 ч.

11. Блокираторы устройств беспроводной связи

11.1. Мозаика

11.1.1. Мозаика 3ДМ

11.1.2. Мозаика Интерьер

11.1.3. Мозаика +

11.1.4. Мозаика (i)

11.2. Дополнительные функции

11.3. Генераторы шума КМ

11.3.1. КМ-3

11.1. МОЗАИКА – 3ДМ.

Устройство предотвращения утечки информации по каналам систем мобильной связи.

Изделие «Мозаика-3ДМ» предназначено для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи. Используется в целях предотвращения утечки информации за пределы выделенного помещения через подслушивающие устройства указанного выше типа, через включенный телефон мобильной связи, а также для обеспечения рабочей обстановки во время проведения переговоров, совещаний и других мероприятиях, требующих тишины.



МОЗАИКА – 3ДМ

Особенности

- работа во всех стандартах сотовой связи;
- простота управления;
- регулировка уровня выходного сигнала, позволяющая ограничить радиус действия изделия в пределах необходимой зоны;
- отсутствие ограничений по продолжительности эксплуатации;
- возможность наращивания дополнительных опций:
 - автономное питание;
 - питание от источника постоянного 12В тока, в том числе бортовой сети автомобиля;
 - установка интеллектуального устройства;
 - установка в атташе-кейс или другие виды аксессуаров для транспортировки;
 - установка дистанционного управления по проводному каналу или инфракрасному каналу;
 - установка направленных антенн;
 - камуфлирование в предметы интерьера и другое.

Технические характеристики

- диапазон рабочих частот: 463-467,5 МГц; 860-960 МГц; 1805-1880 МГц.
- дальность подавления – до 35 метров в радиусе от места установки (в зависимости от близости до базовой станции);
- питание – 220В;
- габариты, мм - 140х190х80.

Устройство соответствует государственным санитарно-эпидемиологическим правилам и нормативам МСанПиН001-96 «Санитарные нормы допустимых уровней физических факторов при применении товаров народного потребления в бытовых условиях» - Заключение государственной санитарно-эпидемиологической службы РФ №77.01.09.650.п.01690.02.5 от 01.02.05г.

11.2. «МОЗАИКА» Интерьер

Устройство предотвращения утечки информации по каналам систем мобильной связи.

Изделия «Мозаика» (Интерьер) предназначено для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM-900/1800, E-GSM, AMPS/DAMPS, CDMA и блокирования работы телефонов названных систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, проведения совещаний. Используется в целях предотвращения утечки информации за пределы выделенного помещения через подслушивающие устройства указанного выше типа, через включенный телефон мобильной связи, а также для обеспечения рабочей обстановки во время проведения переговоров, совещаний



11.2. «МОЗАИКА» Интерьер

Изделие «Мозаика» (Интерьер) не оказывает влияния на работу других технических средств – бытовой электронной техники (теле-, видео-, аудио-, и др.), компьютеров, оргтехники.

Зона эффективного действия изделия зависит от расстояния до ближайшей базовой станции сети мобильной связи и составляет от 3 до 15м.

Для охвата больших площадей используются несколько изделий, разнесенных по защищаемой территории.

Изделие конструктивно исполнено в виде электронных часов и органично вписывается в интерьер помещения.

Электронные часы сохраняют свою работоспособность при работе изделия.

Питание изделия осуществляется от сети 220В.

Изделие соответствует государственным санитарно-эпидемиологическим правилам и нормативам МСанПиН001-96 «Санитарные нормы допустимых уровней физических факторов при применении товаров народного потребления в бытовых условиях» - Заключение государственной санитарно-эпидемиологической службы Российской Федерации N77.01.09.401.п.25558.08.2 от 30.08.2002г.

11.2. МОЗАИКА +

Устройство предотвращения утечки информации

Изделие «Мозаика+» предназначено для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM-900/1800, E-GSM, AMPS/DAMPS, CDMA, NMT-450, IMT-MC(CDMA2000 1x) и блокирования работы телефонов названных систем мобильной связи, блокирования передачи данных с помощью устройств, работающих в стандартах Bluetooth и WiFi.



11.2. МОЗАИКА +

Используется в целях предотвращения утечки информации в пределах радиуса действия устройства через подслушивающие устройства указанного выше типа, через включенный телефон мобильной связи, а также для обеспечения рабочей обстановки во время проведения переговоров, совещаний и других мероприятиях, требующих тишины.

Особенности

- блокирование работы телефонов во всех стандартах сотовой связи;
- расширенные возможности устройства в малогабаритном корпусе – отсутствие аналогов в России и зарубежье;
- простота управления;
- регулировка уровня выходного сигнала, позволяющая ограничить радиус действия изделия в пределах необходимой зоны;
- отсутствие ограничений по продолжительности эксплуатации;
- возможность наращивания дополнительных опций:
 - * автономное питание;
 - * питание от источника постоянного 12В тока, в т.м. числе бортовой сети автомобиля;
 - * установка интеллектуального устройства;

- * установка дистанционного управления по проводному каналу или инфракрасному каналу;
- * монтаж в атташе-кейс или другие типы аксессуаров для транспортировки;
- * камуфлирование в предметы интерьера и другое.

Технические характеристики

- диапазон рабочих частот: 463-467,5 МГц; 869-894 МГц(*); 935-960МГц; 1805-1880 МГц; 2400-2483,5 МГц.
- выходная мощность: в стандартах GSM-900,AMPS/DAMPS,CDMA-800 – не более 2Вт; GSM-1800 – не более 2Вт; NMT-450, IMT-MC(CDMA2000 1x) – не более 2Вт; Bluetooth,WiFi – не более 0,4 Вт;
- дальность подавления – до 45 метров в радиусе от места установки (в зависимости от близости до базовой станции);
- диаграмма направленности антенн – круговая;
- питание – 220В, 50Гц;
- мощность потребляемая - не более 30 Вт;
- габариты, мм – 140x60x190;
- масса, кг – 2,3 кг.

Устройство соответствует государственным санитарно-эпидемиологическим правилам и нормативам СанПиН 2.1.8./2.2.4.1190-03 «Гигиенические требования к размещению и эксплуатации средств сухопутной подвижной радиосвязи», СанПиН 2.2.4.1191-03, СН 2.2.4./2.1.8.562-96 - Заключение государственной санитарно-эпидемиологической службы Российской Федерации №77.01.09.665.п.069746.09.07 от 11.709.2007г.

11.3. МОЗАИКА(i)

Устройство предотвращения утечки информации по каналам систем мобильной связи.

Изделие «Мозаика» (i) предназначено для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM-900/1800, E-GSM, AMPS/DAMPS, CDMA и блокирования работы телефонов названных систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, проведения совещаний. Используется в целях предотвращения утечки информации за пределы выделенного помещения через подслушивающие устройства указанного

выше типа, через включенный телефон мобильной связи, а также для обеспечения рабочей обстановки во время проведения переговоров, совещаний.

Изделие Мозаика (i) не оказывает влияния на работу других технических средств – бытовой электронной техники (теле-, видео-, аудио-, и др.), компьютеров, оргтехники.

Изделие «Мозаика» (i) является интеллектуальным устройством, блокирующая работу сотовых телефонов при появлении хотя бы одного канала связи абонент-базовая станция (в том числе передачу SMS-сообщений).

Зона эффективного действия изделия зависит от расстояния до ближайшей базовой станции сети мобильной связи и составляет от 3 до 15м.

Для регулировки мощности выходного сигнала (для установки оптимальной мощности в зависимости от площади защищаемой территории) имеется регулятор на корпусе изделия.



Мозаика (i)

Для охвата больших площадей используются несколько изделий, разнесенных по защищаемой территории.

Питание изделия осуществляется от сети 220В (через адаптер) или внешнего источника питания 12В.

Изделие соответствует государственным санитарно-эпидемиологическим правилам и нормативам МСанПиН001-96 «Санитарные нормы допустимых уровней физических факторов при применении товаров народного потребления в бытовых условиях» - Заключение государственной санитарно-эпидемиологической службы Российской Федерации N77.01.09.401. п.25558.08.2 от 30.08.2002г.

Дополнительные функции

- Датчик активации устройства при вскрытии корпуса компьютера
- Датчик активации устройства при подъеме корпуса ПК
- Датчик активации устройства при выемке одного контейнера Mobil Rack
- Управление активацией набором специального электронного кода (для устройств серии "Раскат" (Сейф))
- Внутренний монтаж излучателей для устройств серии "Раскат" (ULTRA, ULTRA+) - для каждого диска
- Дополнительный разъем для управления активацией устройства по проводному каналу
- Пульт активации по проводному каналу с контролем целостности линии
- Пульт активации по проводному каналу с контролем целостности линии и активации устройства
- Дополнительный пульт ДУ по радиоканалу (до 50м)
- Демонтаж системы ДУ по радиоканалу (до 50м)
- Усиление системы радио- ДУ до 1000 м (в прямой видимости) с функцией подтверждения об активации
- Дополнительный пульт системы радио- ДУ до 1000 м с функцией подтверждения об активации устройства
- Управление устройством по GSM каналу, активация устройства введением секретного кода, самостоятельная смена Пользователем секретного кода, подтверждение выполнения команды активации.
- Антенна внешняя для GSM-модуля
- Блокировка включения кнопки питания компьютера (включение по идентификатору Touch Memory), два ключа в комплекте.
- Постановка и снятие с охраны механическим ключом
- Постановка и снятие с охраны электронным ключом по идентификатору Touch Memory
- Постановка и снятие с охраны магнитной Proximity Card
- Регистратор событий
- Увеличение продолжительности работы от автономного источника питания до 48 ч.
- Увеличение продолжительности работы от автономного источника питания до 72 ч.
- Питание от источника 12В (для изделий "Мозаика-М", "Мозаика-3", "Мозаика3ДМ")
- Таймер автоматического отключения рабочего режима
- Автономное питание (для изделия "Мозаика")
- Антенна направленная на один диапазон
- Установка блока дистанционного включения по радиоканалу
- Монтаж в атташе-кейсе с автономным питанием
- Монтаж модуля CDMA2000 1X, NMT-450i (для изделия Мозаика-МЦ) с антенной направленной.
- Монтаж интеллектуального устройства (включение при появлении канала связи в пределах защищаемой территории) для двухканальных устройств

11.4. Генераторы шума КМ

11.4.1. КМ-3

Переносное устройство подавления цифровых и кинематических диктофонов и блокирования работы закладных устройств и сотовых телефонов, работающих в стандартах GSM-900/1800, E-GSM, AMPS/DAMPS, CDMA, CDMA2000 1X, NMT-450i. Встроенное в атташе-кейс. Дальность подавления диктофонов - до 3м (в зависимости от типа диктофона). Дальность блокирования устройств, использующих каналы мобильной связи заявленных стандартов - до 25м (в зависимости от места использования относительно базовой станции). Два пульта управления по радиоканалу. Антенны направленные встроенные. Питание 220В; 12В - от встроенных аккумуляторов (время работы - не менее 40 минут от полностью заряженных аккумуляторов); 12В - от автомобильного "прикуривателя" (опция).



КМ-3

12. Оборудование для защиты объектов вычислительной техники от утечки информации

12.1. Генераторы пространственного зашумления

12.1.1. SEL SP -21 Баррикада

12.1.2. ЛГШ-501

12.2. Контроль коммуникаций, индикаторы

12.2.1. Оракул

12.2.2. Оберег

12.3. КПЛ

12.1. Генераторы пространственного зашумления

12.1.1. SEL SP -21 Баррикада

Генератор с регулируемым уровнем излучения SEL SP - 21 "Баррикада" предназначен для маскировки и предупреждения перехвата информативных побочных электромагнитных излучений и наводок от средств вычислительной техники путем создания в широкой полосе частот активных маскирующих помех (типа "белый шум")

Область использования - помещения, в которых расположены средства вычислительной техники с информацией от конфиденциальной до содержащей сведения, составляющие государственную тайну.



Генератор с регулируемым уровнем излучения SEL SP -21 Баррикада

Установка и настройка генератора должны производиться при аттестации объектов информатизации по требованиям безопасности информации организацией, аккредитованной в Государственном реестре системы сертификации средств защиты информации ФСТЭК России.

Устройство генерирует широкополосный шумовой электромагнитный сигнал и обеспечивает:

- Маскировку информативных побочных электромагнитных излучений ПЭВМ и периферийного оборудования.
- Защиту от подслушивающих устройств с радиоканалом мощностью до 5 мВт (без кварцевой стабилизации).

Отличительные особенности:

- малогабаритность;
- наличие двух телескопических антенн позволяют оперативно устанавливать систему и обойтись без прокладки рамочных антенн по периметру помещений;
- возможность работы от сети постоянного тока напряжением 12 В.

SEL SP-21 награжден медалью I степени XI Международного форума "Технологии безопасности-2006" и дипломом XIV международной конференции "Информатизация и информационная безопасность правоохранительных органов"

Изделие имеет сертификаты ФСТЭК (действителен до 22.07.2008) и Минздрава РФ.

Таблица 12.1. - Технические характеристики генератора зашумления SEL SP -21 Баррикада

Диапазон спектра сигнала шума	0,1 - 1800 МГц
Спектральная плотность напряженности электромагнитного поля шума и уровень сигнала на удалении 1 м от излучающих антенн генератора:	
Полоса частот 0,1 - 30,0 МГц	
- полоса пропускания приемника	9 кГц
- спектральная плотность напряженности электромагнитного поля шума	500 не менее мкВ/ м $\sqrt{\text{кГц}}$
- уровень сигнала	не менее 55 дБ/мкВ
Полоса частот 30,0 - 300,0 МГц	
- полоса пропускания приемника	120 кГц
- спектральная плотность напряженности электромагнитного поля шума	не менее 150 мкВ/ м $\sqrt{\text{кГц}}$
- уровень сигнала	не менее 50 дБ/мкВ
Полоса частот 300,0 - 1000,0 МГц	
- полоса пропускания приемника	120 кГц
- спектральная плотность напряженности электромагнитного поля шума	не менее 30 мкВ/ м $\sqrt{\text{кГц}}$
- уровень сигнала	не менее 40 дБ/мкВ
Полоса частот 1000,0 - 1200,0 МГц	
- полоса пропускания приемника	120 кГц
- спектральная плотность напряженности электромагнитного поля шума	не менее 20 мкВ/ м $\sqrt{\text{кГц}}$
- уровень сигнала	не менее 35 дБ/мкВ
Полоса частот 1200,0 - 1800,0 МГц	
- полоса пропускания приемника	120 кГц
- спектральная плотность напряженности электромагнитного поля шума	не менее 5 мкВ/ м $\sqrt{\text{кГц}}$
- уровень сигнала	не менее 20 дБ/мкВ
Энтропийный коэффициент качества шума	не хуже 0,8
Максимальный коэффициент межспектральных корреляционных связей шума	не хуже 1,3
Эффективное значение шума на линейном выходе	не более 15 В
Интегральная регулируемая выходная мощность	0,01 - 4 Вт
Длительность установления рабочего режима	не более 1 с
Электропитание:	
От однофазной сети 220 В	220 В \pm 10% / 50 - 60 Гц
От сети постоянного тока	12 - 14,2 В x 1 А
Условия эксплуатации:	
- температура окружающей среды	от +10 до +40 °С
- относительная влажность воздуха при 25 °С	до 85%
- атмосферн. давление	740 \pm 40 мм рт.ст
Масса генератора (без антенны)	1100 г
Габариты генератора (без антенны)	не более 180x70x30 мм

11.1.2. ЛГШ-501

Генератор радиопомех ЛГШ-501 предназначен для работы в составе системы активной защиты информации (САЗ), обрабатываемой на объектах ЭВТ второй и третьей категорий. САЗ-ЗПЭМИН путем создания широкополосной шумовой электромагнитной помехи в диапазоне частот от 0,01 до 1800 МГц. обеспечивает защиту информации от утечки по каналам.



ЛГШ-501

Принцип работы САЗ на базе генератора ЛГШ-501: создание на границе КЗ шумовой помехи, которая зашумляет побочные излучения защищаемого объекта.

Генератор может работать на две телескопические антенны и (или) на внешние антенны, смонтированные как три короткозамкнутых контура в виде петель из провода, уложенных по периметру трех взаимно перпендикулярных граней.

ЛГШ-501 питается от сети переменного тока напряжением 220 В и частотой 50 Гц. Устройство может эксплуатироваться круглосуточно.

Включение/выключение режима генерации помех производится кнопкой "Сеть" на задней панели устройства.

На передней панели генератора расположен световой индикатор работы.

На задней панели генератора предусмотрен разъем для подключения проводного пульта ДУ (в комплект поставки не входит и изготавливается по месту монтажа).

Установка и настройка генератора производится только специализированной организацией, имеющей соответствующие лицензии Гостехкомиссии России, в рамках проведения работ по аттестации объектов информатизации по требованиям безопасности информации.

Санитарно-эпидемиологическим заключением №78.ДЦ.01.665.П.000106.02.06 от 02.02.06, выданным Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, удостоверяется, что генератор шума ЛГШ-501 соответствует санитарным правилам

СанПиН 2.1.8/2.2.4.1383-03 «Гигиенические требования к размещению и эксплуатации передающих радиотехнических объектов», СанПиН 2.2.4.1191-03 «Электромагнитные поля в производственных условиях».

Таблица 12.2. - Комплект поставки.

Наименование	Количество
Генераторный блок	1
Разъем кабельный PC4TV	2
Руководство по эксплуатации	1
Паспорт	1
Упаковка	1

Внешние антенны и пульт ДУ при необходимости изготавливаются и монтируются на месте и подключаются к генераторному блоку с помощью кабельных разъемов PC4TV. Схемы распайки и монтажа приведены в руководстве по эксплуатации.

Таблица 12.3. - Технические характеристики ЛГШ-501
Уровень сигнала на выходном разъеме генератора в различных диапазонах частот

Диапазон частот	Полоса пропускания	Уровень сигнала
10–150 кГц	200 Гц	не менее 65 дБ
0,15–30 МГц	9 кГц	не менее 85 дБ
30–1000 МГц	120 кГц	не менее 70 дБ
1–1,8 ГГц	120 кГц	не менее 60 дБ

Энтропийный коэффициент качества шума на выходе генератора	не менее 0,8
Количество телескопических антенн	2 шт
Длина телескопической антенны	не менее 70 см
Электропитание	сеть 220 В, 50 Гц
Режим работы	круглосуточно
Средняя наработка на отказ	не менее 10 000 час
Средний срок службы	10 лет
Габаритные размеры генераторного блока	230×100×45 мм
Масса	не более 2 кг

11.2. Контроль коммуникаций, индикаторы

11.2.1. Оракул

Скоростной поисковый приемник-коррелятор SEL SP-81 "Оракул" предназначен для оперативного обнаружения и поиска в ближней зоне устройств съема акустической информации, использующих радиоканал, в т.ч. мобильных телефонов

Наличие пассивного акустического коррелятора позволяет бесшумно и скрытно выявлять источники радиозлучения, модулированные аналоговыми сигналами, (радиомикрофоны) в автоматическом режиме без участия оператора

В приемнике предусмотрены два режима работы: поисковый - для обнаружения и локализации источников радиоизлучений и сторожевой - для непрерывного контроля за радиообстановкой в реальном времени. При обнаружении сигнала индицируются его частота и уровень, а демодулированный сигнал может воспроизводиться через встроенный громкоговоритель. Приемник обнаруживает радиопередатчики с мощностью в антенне 5 мВт на расстоянии не менее 5 м. Время сканирования всего частотного диапазона зависит от помеховой обстановки и составляет в среднем несколько секунд.



Скоростной поисковый приемник - коррелятор SEL SP-81 "Оракул"

Используемый в приборе метод корреляции предназначен для выявления радиомикрофонов и основан на сравнении демодулированного радиосигнала с опорным акустическим, присутствующим в помещении.

Алгоритм, применяемый в приёмнике "Оракул", основан на вычислении кросскорреляционной функции текущей мощности акустического сигнала, т.е. его огибающей. Это позволяет не

учитывать различие формы исследуемого и опорного сигналов, появляющееся из-за резонансных свойств помещения, что существенно повышает достоверность анализа. Для реализации этого алгоритма оптимально подходит именно речевой сигнал, обладающий высоким пик-фактором (т.е. изменением текущей мощности). Кроме того, этот метод позволяет обнаруживать радиопередатчики с закрытым аналоговым каналом, например, с инверсией спектра.

Отличительные особенности:

- сторожевой и поисковый режимы работы;
- встроенный пассивный коррелятор;
- встроенная энергонезависимая память обеспечивает сохранение параметров обнаруженных радиоустройств
- возможность подключения ПК через COM-порт (программное обеспечение приобретается дополнительно).

Программное обеспечение к "Оракулу" позволяет осуществлять полное управление приёмником с портативного компьютера, вести базу данных сигналов, осуществлять просмотр и мониторинг сигналов, а также задавать интересующую частоту сигнала.

Приёмник удостоен медали I степени на VIII международном форуме "Технологии безопасности-2003", медали "Гарантия качества и безопасности" на международном конкурсе "Национальная безопасность-2003", диплома 5-ой межрегиональной выставки "Безопасность. Урал. Поволжье - 2004", золотой медали и диплома сибирской ярмарки "СИББЕЗОПАСНОСТЬ - 2004".

Таблица 12.4. - Технические характеристики SEL SP-81 "Оракул"

диапазон принимаемых частот	20 - 3000 МГц
виды модуляции сигнала	WFM, NFM, AM, импульсная (PM)
стандарты обнаруживаемых цифровых сигналов	D-AMPS, DECT, GSM 900, GSM 1800, Bluetooth
чувствительность по входу для захвата сигнала в диапазоне частот:	
20 - 200 МГц	- 80 дБм (23 мкВ)
200 - 600 МГц	- 70 дБм (71 мкВ)
600 - 1000 МГц	- 63 дБм (160 мкВ)
1000 - 1400 МГц	-56 дБм (360 мкВ)
1400 - 1600 МГц	-49 дБм (795 мкВ)
1600 - 2500 МГц	-46 дБм (1,2 мВ)
2500 - 3000 МГц	- 43 дБм (1,6 мВ)
точка компрессии -1дБ по входу, не менее	-3 дБм
динамический диапазон измерителя уровня сигнала	не менее 70 дБ
время сканирования диапазона	12с
среднее время настройки на один сигнал	3 с
среднее время анализа корреляции одного сигнала	4 с
количество запоминаемых сигналов	до 999
количество исключаемых сигналов	до 999
ток потребления	не более 120 мА
источник питания	батарея 9 В или сеть 220 В через адаптер
дальность обнаружения радиопередатчиков с мощностью в антенне 5 мВт	не менее 5 м
габаритные размеры без антенны	106 х 68 х 32 мм
Масса	250 г

11.2.2. Оберг

Цифровой индикатор поля - частотомер SEL SP-71M "Оберг" создан на основе современных цифровых технологий. Использование микропроцессора, поддерживающего алгоритм работы, обеспечивает практически мгновенное обнаружение в ближней зоне любых радиопередатчиков, интенсивность излучения которых превышает уровень фона на 6-12 дБ, а также обнаружение включенных на передачу сотовых телефонов с возможностью распознавания стандартов GSM и DAMPS.

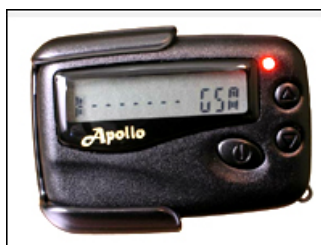
Устройство по использованному корпусу, органам управления и индикации является псевдопейджером и позволяет его обладателю под видом приема пейджерных сообщений получать информацию о наличии в ближней зоне любого устройства с радиоканалом, предназначенного для негласного получения информации, в том числе скрытно включенного сотового телефона.

"Оберег" имеет 3 режима работы:

- сторожевой,
- поисковый и
- настройки параметров.

Отличительные особенности:

- малогабаритность;
- отсутствие внешней антенны;
- реализован алгоритм адаптивного цифрового фильтра для снижения вероятности ложных срабатываний;
- наличие бесшумной индикации (вибровзвонок);
- камуфляж (конструктивно выполнен в корпусе пейджера);
- распознавание сигналов GSM и DAMPS.



Цифровой индикатор поля - частотомер SEL SP-71M "Оберег"

"Оберег" удостоен [диплома II степени выставки "Охрана и безопасность 2001"](#), медали [I степени международного форума "Технологии безопасности-2001"](#) и диплома выставки [MIPS-2003](#)

Таблица 12.5. - Технические характеристики "Оберег"

диапазон частот	100-2800 МГц
дальность обнаружения сотовых телефонов	до 20 м
дальность обнаружения радиомикрофоноов мощностью 5 мВт	до 3 м
динамический диапазон индикатора уровня	не менее 44 дБ
виды индикации	вибровзвонок, световая, звуковая отключаемая
питание	1,5 В (батарея ААА)
время работы в сторожевом режиме	24 часа
время работы в поисковом режиме	24 часа
габариты	60х40х18 мм

КПЛ

Конвертер предназначен для работы совместно со сканирующими приемниками при решении задач выявления сигналов, передаваемых по телефонным проводам и сети 220 В.

Таблица 12.6. - Технические характеристики КПЛ

Диапазон частот	20 кГц - 10 МГц
Частотная характеристика:	
-- 100 кГц	10 дБ
-- 1 МГц	2 дБ
-- 10 МГц	10 дБ

Входы:	
1. сетевой:	
-- рабочее напряжение	0 - 350 В
-- потребляемый ток	не более 10 мА
2. телефонный:	
-- рабочее напряжение	0 - 200 В
-- потребляемый ток	не более 1 мА
Выход	75 О

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Средства от НСД	цена
Система защиты информации от НСД «Страж NT» (версия 2.5)	9850
Система защиты информации от НСД «Страж NT» (версия 3.0)	1125
Электронный ключ Guardant ID (16 Кбайт)	8950

Secret Net автономный вариант:	
Secret Net 5.1 – С	6 950
Плата Secret Net Touch Memory Card	3 126
Считыватель iButton	1 011
Идентификатор DS – 1995	1 001
Установочный комплект Secret Net 5.1	411

Электронный замок «Соболь» в комплекте с идентификаторами DS-1992	8 970
Электронный замок «Соболь» в комплекте с идентификаторами DS-1995	10 300
Электронный замок «Соболь» в комплекте с идентификаторами DS-1996	10 400

Средства от НСД для банка	цена
Secret Net автономный вариант:	8 000
Secret Net 5.1 – С	3 600
Плата Secret Net Touch Memory Card	760
Считыватель iButton	1 100
Идентификатор DS – 1996	520
Установочный комплект Secret Net 5.1	
АПК. Электронный замок «Соболь» в комплекте с идентификаторами DS1996	11375

Программный продукт Secret Net 5.0 (мобильный вариант) (до окончания срока сертификата)	6 900
---	-------

Средства защиты от ПЭМИН и акустической разведки	цена
«Соната – РС1» Устройство защиты сетей электропитания и линиям заземления	14 986
«Соната – РС2» Устройство защиты сетей электропитания и линиям заземления	15 812
«Соната – РК1» Комбинированное устройство защиты объектов информатизации от утечки информации за счет ПЭМИН	16 520
«Соната – Р2» Устройство защиты сетей электропитания и линиям заземления объектов информатизации от утечки информации за счет ПЭМИН	14 278
Дополнительна антенна для «Соната – Р2»	2 596
Соната-АВ, модель 1М Генераторный блок 2-канала 5 октав	16 290
Соната-АВ, модель 3М Генераторный блок 3-канала 7 октав	18 172
ПИ-45 Легкий виброизлучатель 5 октав (для моделей 1М и 3М)	1 534
ВИ-45 Виброизлучатель 5 октав (для моделей 1М и 3М)	1 888
АИ-65 Аудиоизлучатель 5 октав (для моделей 1М и 3М)	1 652
ПИ-3м Легкий виброизлучатель 7 октав (для моделей 3М)	2 006
ВИ-3м Виброизлучатель 7 октав (для моделей 3М)	2 242
АИ-3м Аудиоизлучатель 7 октав (для моделей 3М)	2 714
СА-65М Генератор – аудиоизлучатель 5 октав	2 714
СВ-45М Генератор – виброизлучатель 5 октав	3 186
СП-45М Легкий Генератор – виброизлучатель 5 октав	2 478

Соната-ИП1 Блок питания Генераторов – виброизлучателей	6 608
Соната-ИП2 Блок питания Генераторов – виброизлучателей увеличенной мощности	8 968
Соната-ПРГ1 Модуль "ручного" программирования генераторов-изл. (опция)	13 688
Соната-ПРГ2 Контроллер сопряжения RS232/ReBus для автоматизации конфигурирования и мониторинга (опция).	10 148
Соната-ДУ модель 2mini Аппаратура дистанционного включения комплексов ЗИ.	6 726
Фиксаторы тип 1..5 Фиксаторы для ВИ	190
Фиксатор тип 7 Фиксатор блока «Соната -P2X»	250
Фиксатор тип 8 Фиксатор блока «Соната -P2X»	280
Генератор шума ГШ-2500	12 900
Устройства защиты телефонных аппаратов	
Устройство защиты телефонных аппаратов МП-1А Устройство МП-1А предназначено для защиты телефонного аппарата, подключаемого к аналоговой телефонной линии, от утечки через него речевой информации в режиме ожидания вызова. Исключается утечка от любых источников звука речевого диапазона в помещении, а также съем информации с помощью активных методов воздействия. Устройство обеспечивает два уровня защиты: пассивный и активный. Изделие может устанавливаться в выделенных помещениях до 1 категории включительно. Сертификат № 109 выдан ФСТЭК России.	4000
Устройство защиты телефонных аппаратов МП-1Ц. Устройство МП-1Ц предназначено для защиты телефонного аппарата, подключаемого к цифровой телефонной линии, от утечки через него речевой информации в режиме ожидания вызова. Исключается утечка от любых источников звука речевого диапазона в помещении, а также съем информации с помощью активных методов воздействия. Устройство обеспечивает два уровня защиты: пассивный и активный. Изделие может устанавливаться в выделенных помещениях до 1 категории включительно. Сертификат № 110 выдан ФСТЭК России.	4000
Устройство защиты динамиков систем оповещения МП-5 Устройство защиты МП-5 предназначено для защиты громкоговорителя системы оповещения или однопрограммного приемника системы оповещения от утечки через них акустических сигналов помещения. Устройство обеспечивает защиту при активных методах воздействия. Изделие может устанавливаться в выделенных помещениях до 2 категории включительно. Сертификат № 504/1 ФСТЭК России	4000
Устройство защиты МП-8 ("Сигма-РА") Устройство защиты МП-8 ("Сигма-РА") предназначено для защиты помещений от утечки речевой и другой акустической информации через телефонный аппарат (ТА) в режиме ожидания вызова (при положенной трубке на рычаги ТА) в аналоговых телефонных линиях (ТЛ) телефонного аппарата (ТА), Устройство исключает несанкционированный доступ к электроакустическим преобразователям внутри ТА для дистанционного получения акустической информации из помещения, где он установлен. Устройство обеспечивает защиту при активных методах воздействия. Устройство МП-8 может устанавливаться в выделенных помещениях до 1 категории включительно.	7750
Подавители сотовых телефонов	
"Мозаика-МИНИ" Портативный <u>камуфлированный блокиратор</u> работы сотовых телефонов и накладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 4м. Габариты,мм - 57x85x20. Антенны встроенные. Питание 3В (2 батареи AAA). Автономная работа до 40 минут. Сертификат Минздрава.	12 990
"Мозаика" (ПК) Малогабаритный <u>камуфлированный блокиратор</u> работы сотовых телефонов и накладных устройств, работающих в стандартах GSM-900/1800,AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 10м. Антенны встроенные или внешние. Питание 220В/5В через USB-порт компьютера. Продолжительность непрерывной работы - без ограничений. Габариты, мм - 77x18x127. Сертификат Минздрава.	14 950
"Мозаика" (ПК+) Малогабаритный <u>камуфлированный переносной блокиратор</u> работы сотовых телефонов и накладных устройств, работающих в стандартах GSM-900/1800,AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 10м. Антенны встроенные. Питание 220В/ 5В через USB-порт компьютера/ 5В от встроенного автономного источника питания. Продолжительность непрерывной работы - без ограничений. Автономная работа до 60 минут. Габариты, мм - 77x18x127. Сертификат Минздрава.	16 500
"Мозаика" (Т) (новинка) Портативный <u>камуфлированный блокиратор</u> работы сотовых телефонов и накладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 15м. Антенны встроенные.	18 950

Автономная работа до 90 минут. Габариты,мм - 40x100x18. Сертификат Минздрава Подключение стандарта 3G - UMTS(IMT-2000/WCDMA)	9 950
"Мозаика" (Барсетка) <u>Камуфлированный блокиратор</u> работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 15м (в зависимости от места использования и расстояния до базовой станции). Регулировка уровня выходного сигнала. Питание: 220В; 12В - от автомобильного "прикуривателя"; 12В - от аккумулятора. Продолжительность непрерывной работы без ограничений. Автономная работа до 60 минут. Законченный блок, установленный в кожаную мини-барсетку. Габариты,мм- 230x145x95. Сертификат Минздрава.	34 950
"Мозаика" Блокиратор работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 15м. Регулировка уровня выходного сигнала. Питание: 220В; 12В - от автомобильного "прикуривателя" (опция); 12В - от аккумулятора(опция). Дистанционное управление - проводное(опция), радиоканал(опция), ИК-канал(опция). Габариты,мм 95x158x58. Сертификат Минздрава. Подключение стандарта 3G - UMTS(IMT-2000/WCDMA)	17 900
Монтаж в атташе-кейсе с автономным питанием, питанием от внешнего источника 12В - автомобильного "прикуривателя". Автономная работа до 90 минут.	12 900
"Мозаика" (НЧ) <u>Камуфлированный блокиратор</u> работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Выполнен в виде настольных часов-калькулятора, с полным сохранением их функций. Радиус действия - до 15м. Антенны встроенные. Питание 220В. Габариты,мм 40x140x160. Сертификат Минздрава.	8 900
"Мозаика" (Интерьер) <u>Камуфлированный блокиратор</u> сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Выполнен в виде электронных часов с радиоприемным устройством, с полным сохранением их функций. Радиус действия - до 15м. Антенны встроенные. Питание 220В. Габариты,мм 135x230x40. Сертификат Минздрава. Подключение стандартов CDMA2000 1X, NMT-450i (при сохранении габаритов). Подключение стандарта 3G - UMTS(IMT-2000/WCDMA) (при сохранении габаритов).	19 450
"Мозаика-3" Блокиратор работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*, CDMA2000 1X, NMT-450i. Радиус действия - до 15м. Регулировка уровня выходного сигнала. Питание: 220В; 12В - от автомобильного "прикуривателя"(опция); 12В - от аккумулятора(опция). Дистанционное управление - проводное, радиоканал(опция), ИК-канал(опция). Габариты,мм 140x190x60. Подключение стандарта 3G - UMTS(IMT-2000/WCDMA)	19 950
Монтаж в атташе-кейсе с автономным питанием, питанием от внешнего источника 12В - автомобильного "прикуривателя". Автономная работа до 80 минут.	7950
"Мозаика-М" Блокиратор работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*. Радиус действия - до 30м. Регулировка уровня выходного сигнала. Питание: 220В; 12В - от автомобильного "прикуривателя"(опция); 12В - от аккумулятора(опция). Дистанционное управление - проводное, радиоканал(опция), ИК-канал(опция). Габариты,мм 140x190x60. Подключение стандарта 3G - UMTS(IMT-2000/WCDMA)	12900
Монтаж в атташе-кейсе с автономным питанием, питанием от внешнего источника 12В - автомобильного "прикуривателя". Автономная работа до 70 минут.	25 900
"Мозаика-3ДМ" Блокиратор работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*, CDMA2000 1X, NMT-450i. Радиус действия - до 30м. Регулировка уровня выходного сигнала. Питание: 220В; 12В - от автомобильного "прикуривателя"(опция); 12В - от аккумулятора(опция). Дистанционное управление - проводное, радиоканал(опция), ИК-канал(опция). Габариты,мм 140x190x80. Сертификат Минздрава. Монтаж в атташе-кейсе с автономным питанием, питанием от внешнего источника 12В - автомобильного "прикуривателя". Автономная работа до 60 минут.	13 900
"Мозаика+" Блокиратор работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*, CDMA2000 1X, NMT-450i, Bluetooth,WiFi . Радиус действия - до 40м. Регулировка уровня выходного сигнала.	8 900
	29 950
	18 900
	9 200
	45 550
	9 200
	54 950

Питание: 220В; 12В - от автомобильного "прикуривателя"(опция); 12В - от аккумулятора(опция). Дистанционное управление - проводное, радиоканал(опция), ИК-канал(опция). Габариты,мм 140х190х60. Сертификат Минздрава.	
"Мозаика-Д" Блокиратор работы сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, MPS/DAMPS*,CDMA-800*,E-GSM*.Радиус действия - до 50м. Регулировка уровня выходного сигнала. Антенны кругового или направленного(опция) действия. Питание: 220В; 12В - от автомобильного "прикуривателя"(опция); 12В - от аккумулятора(опция). Дистанционное управление - проводное, радиоканал(опция), ИК-канал(опция). Габариты,мм 280х240х130. Предназначен для длительной непрерывной эксплуатации в условиях непосредственной близости соты.	49 950
"Мозаика-МЦ" Камуфлированный блокиратор сотовых телефонов и закладных устройств, работающих в стандартах GSM-900/1800, AMPS/DAMPS*,CDMA-800*,E-GSM*, CDMA2000 1X, NMT-450i, Bluetooth и WiFi(опция), а также UMTS(W-CDMA) - стандарте третьего поколения 3G(опция). Выполнен в корпусе музыкального центра с полным сохранением его работоспособности. Радиус действия - до 50м. Регулировка уровня выходного сигнала. Антенны встроенные направленные. Дистанционное управление – проводное (опция), радиоканал(опция), ИК-канал(опция). Питание 220В. Продолжительность непрерывной работы - без ограничений. Габариты,мм 95х158х58.	65 450

ЛГШ-301: акустический генератор шума	6 200
ЛГШ-221: генератор шума для сети 220В	15 400
ЛГШ-402: генератор виброакустического шума	10 000
ЛГШ-403: генератор виброакустического шума	4 500
ЛВП-2о, -2т,-2с: сертифицированные	2 200
ЛГШ-404: генератор виброакустического шума	23 580
ЛФС-10-1Ф:сетевой фильтр для максимальной нагрузки до 10А	15 800
ЛФС-40-1Ф: сетевой фильтр для максимальной нагрузки 40 А	25 000
«Гранит-8»: абонентское устройство защиты телефонных линий	1 500
ЛГШ-501: генератор радиопомех для защиты от ПЭМИН	15 400
ЛГШ-503: генератор радиопомех для защиты от ПЭМИН и по сети 220 В	14 500
ЛГШ-701: подавитель сотовой связи	51 700
ЛГШ-701+:подавитель сотовой связи с комплектом выносных антенн	69 000
ЛГШ-701-АВН: комплект выносных направленных антенн	28 000
ЛГШ-702: подавитель Bluetooth и WiFi	30 800
ЛГШ-703:подавитель 3G	50 000
ЛФС-40-1ФТРИО	70 000
ЛГШ-712:	20 000
ЛГШ-713:	25 000
ЛГШ-714	29 500
ЛГШ-715	49 900
ЛГШ-716	65 000

Цены могут меняться производителем, уточнять в отделе продаж.

Цены указаны без учета доставки.

http://builder-c.narod.ru/user/atak_72.htm

7.2. ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ ЗАЩИТЫ ОТ УДАЛЕННЫХ АТАК В СЕТИ INTERNET

К программно-аппаратным средствам обеспечения информационной безопасности средств связи в вычислительных сетях относятся:

- аппаратные шифраторы сетевого трафика;
- методика Firewall, реализуемая на базе программно-аппаратных средств;
- защищенные сетевые криптопротоколы;
- программно-аппаратные анализаторы сетевого трафика;
- защищенные сетевые ОС.

Существует огромное количество литературы, посвященной этим средствам защиты, предназначенным для использования в сети Internet (за последние два года практически в каждом номере любого компьютерного журнала можно найти статьи на эту тему).

Далее мы, по возможности кратко, чтобы не повторять всем хорошо известную информацию, опишем данные средства защиты, применяемые в Internet. При этом мы преследуем следующие цели:

во-первых, еще раз вернемся к мифу об "абсолютной защите", которую якобы обеспечивают системы Firewall, очевидно, благодаря стараниям их продавцов;

во-вторых, сравним существующие версии криптопротоколов, применяемых в Internet, и дадим оценку, по сути, критическому положению в этой области; и,

в-третьих, ознакомим читателей с возможностью защиты с помощью сетевого монитора безопасности, предназначенного для осуществления динамического контроля за возникающими в защищаемом сегменте IP-сети ситуациями, свидетельствующими об осуществлении на данный сегмент одной из описанных в 4 главе удаленных атак.

7.2.1. Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети

В общем случае методика Firewall реализует следующие основные три функции:

1. Многоуровневая фильтрация сетевого трафика.

Фильтрация обычно осуществляется на трех уровнях OSI:

- сетевом (IP);
- транспортном (TCP, UDP);
- прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация сетевого трафика является основной функцией систем Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику безопасности в выделенном сегменте IP-сети, то есть, настроив соответствующим образом Firewall, можно разрешить или запретить пользователям, как доступ из внешней сети к соответствующим службам хостов или к хостам, находящимся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Можно провести аналогию с администратором локальной ОС, который для осуществления политики безопасности в системе назначает необходимым образом соответствующие отношения между субъектами (пользователями) и объектами системы (файлами, например), что позволяет разграничить доступ субъектов системы к ее объектам в соответствии с заданными администратором правами доступа. Те же рассуждения применимы к Firewall-фильтрации: в качестве субъектов взаимодействия будут выступать IP-адреса хостов пользователей, а в качестве объектов, доступ к которым необходимо разграничить, - IP-адреса хостов, используемые транспортные протоколы и службы предоставления удаленного доступа.

2. Проxy-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте.

Проxy-схема позволяет, во-первых, при доступе к защищенному Firewall сегменту сети осуществить на нем дополнительную идентификацию и аутентификацию удаленного пользователя и, во-вторых, является основой для создания частных сетей с виртуальными IP-адресами. Смысл проxy-схемы состоит в создании соединения с конечным адресатом через промежуточный проxy-сервер (*проxy* от англ. *полномочный*) на хосте Firewall. На этом проxy-сервере и может осуществляться дополнительная идентификация абонента.

3. Создание частных сетей (Private Virtual Network - PVN) с "виртуальными" IP-адресами (NAT - Network Address Translation).

В том случае, если администратор безопасности сети считает целесообразным скрыть истинную топологию своей внутренней IP-сети, то ему можно порекомендовать использовать системы Firewall для создания частной сети (PVN-сеть). Хостам в PVN-сети назначаются любые "виртуальные" IP-адреса. Для адресации во внешнюю сеть (через Firewall) необходимо либо использование на хосте Firewall описанных выше проxy-серверов, либо применение специальных систем роутинга (маршрутизации), только через которые и возможна внешняя адреса-

ция. Это происходит из-за того, что используемый во внутренней PVN-сети виртуальный IP-адрес, очевидно, не пригоден для внешней адресации (внешняя адресация - это адресация к абонентам, находящимся за пределами PVN-сети). Поэтому проху-сервер или средство роутинга должно осуществлять связь с абонентами из внешней сети со своего настоящего IP-адреса. Кстати, эта схема удобна в том случае, если вам для создания IP-сети выделили недостаточное количество IP-адресов (в стандарте IPv4 это случается, сплошь и рядом, поэтому для создания полноценной IP-сети с использованием проху-схемы достаточно только одного выделенного IP-адреса для проху-сервера).

Итак, любое устройство, реализующее хотя бы одну из этих функций Firewall-методики, и является Firewall-устройством. Например, ничто не мешает вам использовать в качестве Firewall-хоста компьютер с обычной ОС FreeBSD или Linux, у которой соответствующим образом необходимо скомпилировать ядро ОС. Firewall такого типа будет обеспечивать только многоуровневую фильтрацию IP-трафика. Другое дело, предлагаемые на рынке мощные Firewall-комплексы, сделанные на базе ЭВМ или мини-ЭВМ, обычно реализуют все функции Firewall-методики и являются полнофункциональными системами Firewall. На следующем рисунке изображен сегмент сети, отделенный от внешней сети полнофункциональным Firewall-хостом.

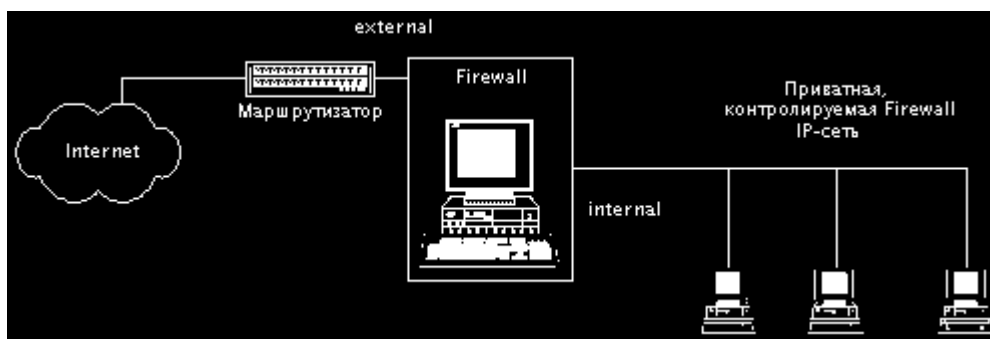


Рис.1. Фрагмент сети, отделенный от внешней сети полнофункциональным Firewall-хостом

Однако администраторам IP-сетей, поддавшись на рекламу систем Firewall, не стоит заблуждаться на тот счет, что Firewall это гарантия абсолютной защиты от удаленных атак в сети Internet. Firewall - не столько средство обеспечения безопасности, сколько возможность централизованно осуществлять сетевую политику разграничения удаленного доступа к доступным ресурсам вашей сети. Да, в том случае, если, например, к данному хосту запрещен удаленный TELNET-доступ, то Firewall однозначно предотвратит возможность данного доступа. Но дело в том, что большинство удаленных атак имеют совершенно другие цели (бессмысленно пытаться получить определенный вид доступа, если он запрещен системой Firewall). Действительно, зададим себе вопрос, а какие из рассмотренных в 4 главе удаленных атак может предотвратить Firewall? Анализ сетевого трафика (п. 4.1)? Очевидно, нет! Ложный ARP-сервер (п. 4.2)? И да, и нет (для защиты вовсе не обязательно использовать Firewall). Ложный DNS-сервер (п. 4.3)? Нет, к сожалению, Firewall вам тут не помощник. Навязывание ложного маршрута при помощи протокола ICMP (п. 4.4)? Да, эту атаку путем фильтрации ICMP-сообщений Firewall легко отразит (хотя достаточно будет фильтрующего маршрутизатора, например Cisco). Подмена одного из субъектов TCP-соединения (п. 4.5)? Ответ отрицательный; Firewall тут абсолютно не при чем. Нарушение работоспособности хоста путем создания направленного шторма ложных запросов или переполнения очереди запросов (п. 4.6)? В этом случае применение Firewall только ухудшит все дело. Атакующему для того, чтобы вывести из строя (отрезать от внешнего мира) все хосты внутри защищенного Firewall-системой сегмента, достаточно атаковать только один Firewall, а не несколько хостов (это легко объясняется тем, что связь внутренних хостов с внешним миром возможна только через Firewall).

Из всего вышесказанного отнюдь не следует, что использование систем Firewall абсолютно бессмысленно. Нет, на данный момент этой методике (именно как методике!) нет альтернативы. Однако надо четко понимать и помнить ее основное назначение. Нам представляется, что применение методики Firewall для обеспечения сетевой безопасности является необходимым,

но *отнюдь не достаточным* условием, и не нужно считать, что, поставив Firewall, вы разом решите все проблемы с сетевой безопасностью и избавитесь от всех возможных удаленных атак из сети Internet. Прогнившую с точки зрения безопасности сеть Internet никаким отдельно взятым Firewall'ом не защитишь!

7.2.2. Программные методы защиты, применяемые в сети Internet

К программным методам защиты в сети Internet можно отнести прежде всего защищенные криптопротоколы, с использованием которых появляется возможность надежной защиты соединения. В следующем пункте пойдет речь о существующих на сегодняшний день в Internet подходах и основных, уже разработанных, криптопротоколах.

К иному классу программных методов защиты от удаленных атак относятся существующие на сегодняшний день программы, основная цель которых - анализ сетевого трафика на предмет наличия одного из известных активных удаленных воздействий. Об этом пункт 7.2.2.2.

7.2.2.1. SKIP-технология и криптопротоколы SSL, S-HTTP как основное средство защиты соединения и передаваемых данных в сети Internet

Прочитав 4 и 5 главы, читатель, очевидно, уяснил, что одна из основных причин успеха удаленных атак на распределенные ВС кроется в использовании сетевых протоколов обмена, которые не могут надежно идентифицировать удаленные объекты, защитить соединение и передаваемые по нему данные. Поэтому совершенно естественно, что в процессе функционирования Internet были созданы различные защищенные сетевые протоколы, использующие криптографию как с закрытым, так и с открытым ключом. Классическая криптография с симметричными криптоалгоритмами предполагает наличие у передающей и принимающей стороны симметричных (одинаковых) ключей для шифрования и дешифрирования сообщений. Эти ключи предполагается распределить заранее между конечным числом абонентов, что в криптографии называется стандартной проблемой статического распределения ключей. Очевидно, что применение классической криптографии с симметричными ключами возможно лишь на ограниченном множестве объектов. В сети Internet для всех ее пользователей решить проблему статического распределения ключей, очевидно, не представляется возможным. Однако одним из первых защищенных протоколов обмена в Internet был протокол Kerberos, основанный именно на статическом распределении ключей для конечного числа абонентов. Таким же путем, используя классическую симметричную криптографию, вынуждены идти наши спецслужбы, разрабатывающие свои защищенные криптопротоколы для сети Internet. Это объясняется тем, что почему-то до сих пор нет гостированного криптоалгоритма с открытым ключом. Везде в мире подобные стандарты шифрования давно приняты и сертифицированы, а мы, видимо, опять идем другим путем!

Итак, понятно, что для того, чтобы дать возможность защититься всему множеству пользователей сети Internet, а не ограниченному его подмножеству, необходимо использовать динамически вырабатываемые в процессе создания виртуального соединения ключи при использовании криптографии с открытым ключом (п. 6.2 и подробно в [11]). Далее мы рассмотрим основные на сегодняшний день подходы и протоколы, обеспечивающие защиту соединения.

SKIP (Secure Key Internet Protocol)-технологией называется стандарт инкапсуляции IP-пакетов, позволяющий в существующем стандарте IPv4 на сетевом уровне обеспечить защиту соединения и передаваемых по нему данных. Это достигается следующим образом: SKIP-пакет представляет собой обычный IP-пакет, поле данных которого представляет из себя SKIP-заголовок определенной спецификацией формата и криптограмму (зашифрованные данные). Такая структура SKIP-пакета позволяет беспрепятственно направлять его любому хосту в сети Internet (межсетевая адресация происходит по обычному IP-заголовку в SKIP-пакете). Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму расшифровывает криптограмму и формирует обычный TCP- или UDP-пакет, который и передает соответствующему обычному модулю (TCP или UDP) ядра операционной системы. В принципе, ничто не мешает разработчику формировать по данной схеме свой оригинальный заголовок, отличный от SKIP-заголовка.

S-HTTP (Secure HTTP) - это разработанный компанией Enterprise Integration Technologies (EIT) специально для Web защищенный HTTP-протокол. Протокол S-HTTP позволяет обеспечить надежную криптозащиту *только* HTTP-документов Web-севера и функционирует на прикладном уровне модели OSI. Эта особенность протокола S-HTTP делает его абсолютно специализированным средством защиты соединения, и, как следствие, невозможное его применение для защиты всех остальных прикладных протоколов (FTP, TELNET, SMTP и др.). Кроме того, ни один из существующих на сегодняшний день основных Web-броузеров (ни Netscape Navigator 3.0, ни Microsoft Explorer 3.0) не поддерживают данный протокол.

SSL (Secure Socket Layer) - разработка компании Netscape - *универсальный* протокол защиты соединения, функционирующий на сеансовом уровне OSI. Этот протокол, использующий криптографию с открытым ключом, на сегодняшний день, по нашему мнению, является единственным универсальным средством, позволяющим динамически защитить любое соединение с использованием любого прикладного протокола (DNS, FTP, TELNET, SMTP и т. д.). Это связано с тем, что SSL, в отличие от S-HTTP, функционирует на промежуточном сеансовом уровне OSI (между транспортным - TCP, UDP, - и прикладным - FTP, TELNET и т. д.). При этом процесс создания виртуального SSL-соединения происходит по схеме Диффи и Хеллмана (п. 6.2), которая позволяет выработать криптостойкий сеансовый ключ, используемый в дальнейшем абонентами SSL-соединения для шифрования передаваемых сообщений. Протокол SSL сегодня уже практически оформился в качестве официального стандарта защиты для HTTP-соединений, то есть для защиты Web-серверов. Его поддерживают, естественно, Netscape Navigator 3.0 и, как ни странно, Microsoft Explorer 3.0 (вспомним ту ожесточенную войну броузеров между компаниями Netscape и Microsoft). Конечно, для установления SSL-соединения с Web-сервером еще необходимо и наличие Web-сервера, поддерживающего SSL. Такие версии Web-серверов уже существуют (SSL-Apache, например). В заключении разговора о протоколе SSL нельзя не отметить следующий факт: законами США до недавнего времени был запрещен экспорт криптосистем с длиной ключа более 40 бит (недавно он был увеличен до 56 бит). Поэтому в существующих версиях броузеров используются именно 40-битные ключи. Криптоаналитиками путем экспериментов было выяснено, что в имеющейся версии протокола SSL шифрование с использованием 40-битного ключа не является надежной защитой для передаваемых по сети сообщений, так как путем простого перебора (2^{40} комбинаций) этот ключ подбирается за время от 1,5 (на суперЭВМ Silicon Graphics) до 7 суток (в процессе вычислений использовалось 120 рабочих станций и несколько мини ЭВМ).

Итак, очевидно, что повсеместное применение этих защищенных протоколов обмена, особенно SSL (конечно, с длиной ключа более 40 бит), поставит надежный барьер на пути всевозможных удаленных атак и серьезно усложнит жизнь кракеров всего мира. *Однако весь трагизм сегодняшней ситуации с обеспечением безопасности в Internet состоит в том, что пока ни один из существующих криптопротоколов (а их уже немало) не оформился в качестве единого стандарта защиты соединения, который поддерживался бы всеми производителями сетевых ОС!* Протокол SSL, из имеющихся на сегодня, подходит на эту роль наилучшим образом. Если бы его поддерживали все сетевые ОС, то не потребовалось бы создание специальных прикладных SSL-совместимых серверов (DNS, FTP, TELNET, WWW и др.). Если не договориться о принятии единого стандарта на защищенный протокол сеансового уровня, то тогда потребуются принятие многих стандартов на защиту каждой отдельной прикладной службы. Например, уже разработан экспериментальный, никем не поддерживаемый протокол Secure DNS. Также существуют экспериментальные SSL-совместимые Secure FTP- и TELNET-серверы. Но все это без принятия единого поддерживаемого всеми производителями стандарта на защищенный протокол не имеет абсолютно никакого смысла. А на сегодняшний день производители сетевых ОС не могут договориться о единой позиции на эту тему и, тем самым, перекладывают решение этих проблем непосредственно на пользователей Internet и предлагают им решать *свои* проблемы с информационной безопасностью так, как тем заблагорассудится!

7.2.2.2. Сетевой монитор безопасности IP Alert-1

Практические и теоретические изыскания авторов, по направлению, связанному с исследованием безопасности распределенных ВС, в том числе и сети Internet (два полярных направления исследования: нарушение и обеспечение информационной безопасности), навели на следующую мысль: в сети Internet, как и в других сетях (например, Novell NetWare, Windows NT), ощущается серьезная нехватка программного средства защиты, осуществляющего **комплексный** контроль (мониторинг) на канальном уровне за всем потоком передаваемой по сети информации с целью обнаружения всех типов удаленных воздействий, описанных в 4 главе. Исследование рынка программного обеспечения сетевых средств защиты для Internet выявило тот факт, что подобных комплексных средств обнаружения удаленных воздействий по нашим сведениям не существует, а те, что имеются, предназначены для обнаружения воздействий одного конкретного типа (например, ICMP Redirect (п. 4.4) или ARP (п. 4.2)). Поэтому и была начата разработка средства контроля сегмента IP-сети, предназначенного для использования в сети Internet и получившее следующее название: сетевой монитор безопасности **IP Alert-1**. Основная задача этого средства, программно анализирующего сетевой трафик в канале передачи, состоит не в отражении осуществляемых по каналу связи удаленных атак, а в их обнаружении, протоколировании (ведении файла аудита с протоколированием в удобной для последующего визуального анализа форме всех событий, связанных с удаленными атаками на данный сегмент сети) и незамедлительным сигнализированием администратору безопасности в случае обнаружения удаленной атаки. *Основной задачей* сетевого монитора безопасности **IP Alert-1** является *осуществление контроля* за безопасностью соответствующего сегмента сети Internet.

Сетевой монитор безопасности **IP Alert-1** обладает следующими функциональными возможностями и позволяет, путем сетевого анализа, обнаружить следующие удаленные атаки на контролируемый им сегмент сети Internet.

Функциональные возможности сетевого монитора безопасности IP Alert-1

1. Контроль за соответствием IP- и Ethernet-адресов в пакетах, передаваемых хостами, находящимися внутри контролируемого сегмента сети.

На хосте IP Alert-1 администратор безопасности создает статическую ARP-таблицу, куда заносит сведения о соответствующих IP- и Ethernet-адресах хостов, находящихся внутри контролируемого сегмента сети.

Данная функция позволяет обнаружить несанкционированное изменение IP-адреса или его подмену (IP Spoofing).

2. Контроль за корректным использованием механизма удаленного ARP-поиска.

Эта функция позволяет, используя статическую ARP-таблицу, определить удаленную атаку "Ложный ARP-сервер" (п. 4.2).

3. Контроль за корректным использованием механизма удаленного DNS-поиска.

Эта функция позволяет определить все возможные виды удаленных атак на службу DNS (атаки в п. 4.3. 1- 4.3.3).

4. Контроль на наличие ICMP Redirect сообщения.

Данная функция оповещает об обнаружении ICMP Redirect сообщения и соответствующей удаленной атаки, описанной в п. 4.4

5. Контроль за корректностью попыток удаленного подключения путем анализа передаваемых запросов.

Эта функция позволяет обнаружить,

- во-первых, попытку исследования закона изменения начального значения идентификатора TCP-соединения - ISN (п. 4.5.1),

- во-вторых, удаленную атаку "отказ в обслуживании", осуществляемую путем переполнения очереди запросов на подключение (п. 4.6), и,

- в-третьих, направленный "шторм" ложных запросов на подключение (как TCP, так и UDP), приводящий также к отказу в обслуживании (п. 4.6).

Таким образом, сетевой монитор безопасности IP Alert-1 позволяет обнаружить, оповестить и запротолировать все виды удаленных атак, описанных в 4 главе! При этом данная программа никоим образом не является конкурентом системам Firewall. **IP Alert-1**, используя

описанные и систематизированные в 4 главе особенности удаленных атак на сеть Internet, служит необходимым дополнением - кстати, несравнимо более дешевым, - к системам Firewall. Без монитора безопасности большинство попыток осуществления удаленных атак на ваш сегмент сети останется скрыто от ваших глаз. Ни один из известных авторов файрволов не занимается подобным интеллектуальным анализом проходящих по сети сообщений на предмет выявления различного рода удаленных атак, ограничиваясь, в лучшем случае, ведением журнала, в который заносятся сведения о попытках подбора паролей для TELNET и FTP, о сканировании портов и о сканировании сети с использованием знаменитой программы удаленного поиска известных уязвимостей сетевых ОС - SATAN (п. 8.9.1). Поэтому, если администратор IP-сети не желает оставаться безучастным и довольствоваться ролью простого статиста при удаленных атаках на его сеть, то ему желательно использовать сетевой монитор безопасности **IP Alert-1**. Кстати, напомним, что Цутому Шимомура смог запротоколировать атаку Кевина Митника (п. 4.5.2), во многом, видимо, благодаря программе tcpdump - простейшему анализатору IP-трафика.

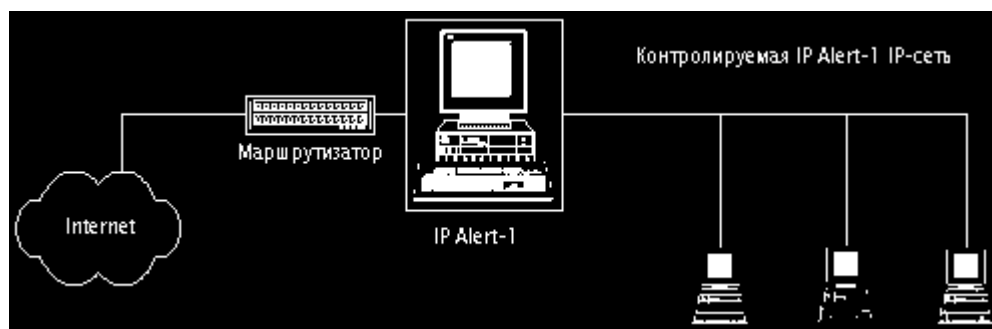


Рис.1. Комплексное использование полнофункционального Firewall-хостом с IP Alert-1

<http://www.zahist.narod.ru/paparazzi.htm>

ОБЗОР ПРОГРАММНЫХ СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НАБЛЮДЕНИЯ ЗА ПЕРСОНАЛОМ

УДК 004.056.5

Безмальный В.Ф.

Введение

Технологии наблюдаемости и основные требования к ним

StatWin 5.0

Invisible Activity Spy Config v2.3

Inlook Express Control Panel

PC Spy Present Softdd v2.31

Paparazzi Industar Cybernetics Corp. 1999-2000 г.

Выводы

Введение

Наиболее уязвимым элементом любой компьютерной системы (и наибольшей угрозой для компьютерной безопасности) является персонал. Некоторые люди могут быть просто неподготовленными: они способны невольно уничтожить важную информацию, которая хранится в системе, или вмешаться в работу системы. Другие могут умышленно нарушать правила и использовать компьютер для личных целей. Существуют также истинные преступники, которые воруют данные (или сами компьютеры) либо намеренно наносят ущерб компьютерному объекту [1].

Защита от персонала - это большая проблема, которой в настоящее время уделяется огромное внимание во всем мире. **По сведениям некоторых зарубежных агентств до 90% всех нарушений информационной защиты осуществляется настоящими или бывшими сотрудниками потерпевших фирм.** В Украине эта проблема стоит особенно остро, так как от-

сутствие специализированных технических средств и программного обеспечения, а также некомпетентность ответственных лиц, создают благоприятную почву для развития различных форм промышленного и коммерческого шпионажа.

Объектом промышленного шпионажа обычно выступает конфиденциальная информация, составляющая коммерческую тайну. Субъектами промышленного шпионажа, как в форме незаконного сбора конфиденциальной информации, так и в форме ее незаконного использования, являются лица, которые (или с помощью которых) реализуют внешние угрозы (конкуренты, агенты конкурентов, партнеры и др.) или внутренние угрозы (сотрудники) информационной безопасности субъектов предпринимательской деятельности. При этом обязательным признаком объективной стороны незаконного использования сведений, содержащих коммерческую тайну, являются большие материальные убытки субъекта предпринимательской деятельности, т. е. убытки, которые в 50 и более раз превышают установленный законом необлагаемый минимум доходов граждан в месяц [1].

В программах защиты от персонала (Personnel Security Programs) используется два основных подхода.

Первый связан с разработкой правил безопасного использования компьютеров при работе в сети, разграничением доступа к информации и т.д., а также разработкой физических мер защиты (охрана помещений, применение систем наблюдения и т.д.).

Второй подход связан с определением состава программного (программно-аппаратного) обеспечения, которое используется администратором безопасности вычислительной системы для обеспечения ее наблюдаемости. Т.е. свойства вычислительной системы, позволяющего фиксировать деятельность пользователей и процессов, использование пассивных объектов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и/или обеспечения ответственности за определенные действия [1]. Именно это свойство, в зависимости от качества его реализации, позволяет в той или иной мере контролировать соблюдение сотрудниками предприятия установленных правил безопасной работы на компьютерах.

Однако многие предприятия Украины часто ограничиваются какой-либо одной мерой защиты, например, покупкой дорогостоящего межсетевого экрана, работающего на границе внутренней корпоративной сети и внешней глобальной сети Internet. При этом предполагается, что все компьютеры, объединенные в сеть, имеют выход в Internet через этот межсетевой экран. Между тем, крупнейшие корпорации мира ежегодно увольняют сотни сотрудников за то, что те приносят свои модемы и подключаются к внешней сети через телефонные линии со своих рабочих мест. Если произошла утечка критичной информации, то администратор безопасности, не имея дополнительных программных средств, практически не в состоянии выявить злоумышленника и определить, к какому компьютеру, в какое время был несанкционированно подключен модем, и какая именно информация была скомпрометирована. С этой точки зрения, межсетевые экраны не могут обеспечить надежную защиту от персонала.

Другой пример - некоторые сотрудники банков могут за определенную плату совершать незаконную деятельность, предоставляя заинтересованным лицам сведения о финансовых операциях любых клиентов банка. Эти сведения могут передаваться заинтересованному лицу, как по сети, так и в виде распечатки, сделанной на локальном принтере. Во втором случае никакие средства сетевого контроля не в состоянии выявить нарушение.

Для решения этих и многих других проблем, связанных с защитой от персонала, необходимо применять программные или программно-аппаратные средства, реализующие свойство наблюдаемости вычислительных систем, что позволяет:

- определить (локализовать) все случаи попыток несанкционированного доступа к конфиденциальной информации с точным указанием времени и сетевого рабочего места, с которого такая попытка осуществлялась. Локализовать все случаи искажения (уничтожения) информации;
- определить факты несанкционированной установки программного обеспечения;

- проконтролировать возможность использования персональных компьютеров в нерабочее время и выявить цель такого использования;
- определить все случаи несанкционированного использования модемов в локальной сети путем анализа фактов запуска несанкционированно установленных специализированных приложений;
- определить все случаи набора на клавиатуре критичных слов и словосочетаний, подготовки каких-либо критичных документов, передача которых третьим лицам приведет к материальному ущербу;
- определить факты нецелевого использования персональных компьютеров и т.д.

Технологии наблюдаемости и основные требования к ним

Рассмотрим ряд технических требований, которым должны удовлетворять программные или программно-аппаратные средства, обеспечивающие наблюдаемость автоматизированных систем (АС), т.е. организационно-технических систем, реализующих информационную технологию и объединяющих вычислительные системы, физическую среду, персонал и обрабатываемую информацию. Под вычислительной системой (ВС) подразумевается совокупность программно-аппаратных средств, предназначенных для обработки информации.

Программы, обеспечивающие наблюдаемость ВС, выполняются с использованием технологии "клиент-сервер".

Существует одна серверная часть и ограниченное множество клиентских частей.

Клиентские части устанавливаются на рабочие станции конечных пользователей, которые могут работать под управлением различных операционных систем.

Основные функции клиентской части:

- регистрация определенных событий;
- ведение журнала регистрации;
- передача журнала регистрации на серверную часть по установленному администратором безопасности критерию.

Клиентская часть должна:

- загружаться автоматически с загрузкой операционной системы;
- быть невидимой для пользователя;
- регистрировать тексты, набираемые в графических и консольных окнах;
- регистрировать время, дату загрузки системы, имя текущего пользователя;
- регистрировать время и дату запускаемых приложений;
- регистрировать время и дату переключения между задачами;
- регистрировать адреса посещаемых узлов Internet;
- иметь возможность применения фильтров для контроля строго определенных приложений;
- иметь возможность контроля по расписанию;
- быть устойчивой к воздействию пользователя;
- передавать отчетную информацию на серверную часть невидимо для пользователя;
- использовать как можно меньше системных ресурсов, не оказывая заметного влияния на производительность системы;
- иметь возможность автоматизированной установки в локальной сети;
- не конфликтовать с антивирусным и другим программным обеспечением;
- и др.

Таким образом, клиентская часть собирает подробные сведения о том, какие действия производились пользователем на компьютере.

Рассмотрим более подробно существующее программное обеспечение, решающее данную проблему на примере следующих программ:

1. StatWin 5.0, автор Дворак В.В. Программа работает под управлением Windows 95/98/NT/2000. (<http://statwin-r.da.ru>).
2. Invisible Activity Spy Config v2.3 Разработка Alin Inclezan (<http://www.geocities.com/SiliconValley/Station/2980/ias.html>).

3. Inlook Express Control Panel (<http://www.Jungle-Monkey.com>)
4. PC Spy Present Softdd v2.31 (<http://www.softdd.com>)
5. Paparazzi Industar Cybernetics Corp. 1999-2000г. ([http://www.xakep.ru/post/10845/default .asp](http://www.xakep.ru/post/10845/default.asp)) StatWin 5.0

StatWin 5.0

Инсталляционный модуль программы занимает 800kb. Программа состоит из двух модулей ExecStat.exe и SeeStat.exe, назначение которых понятно из названия.

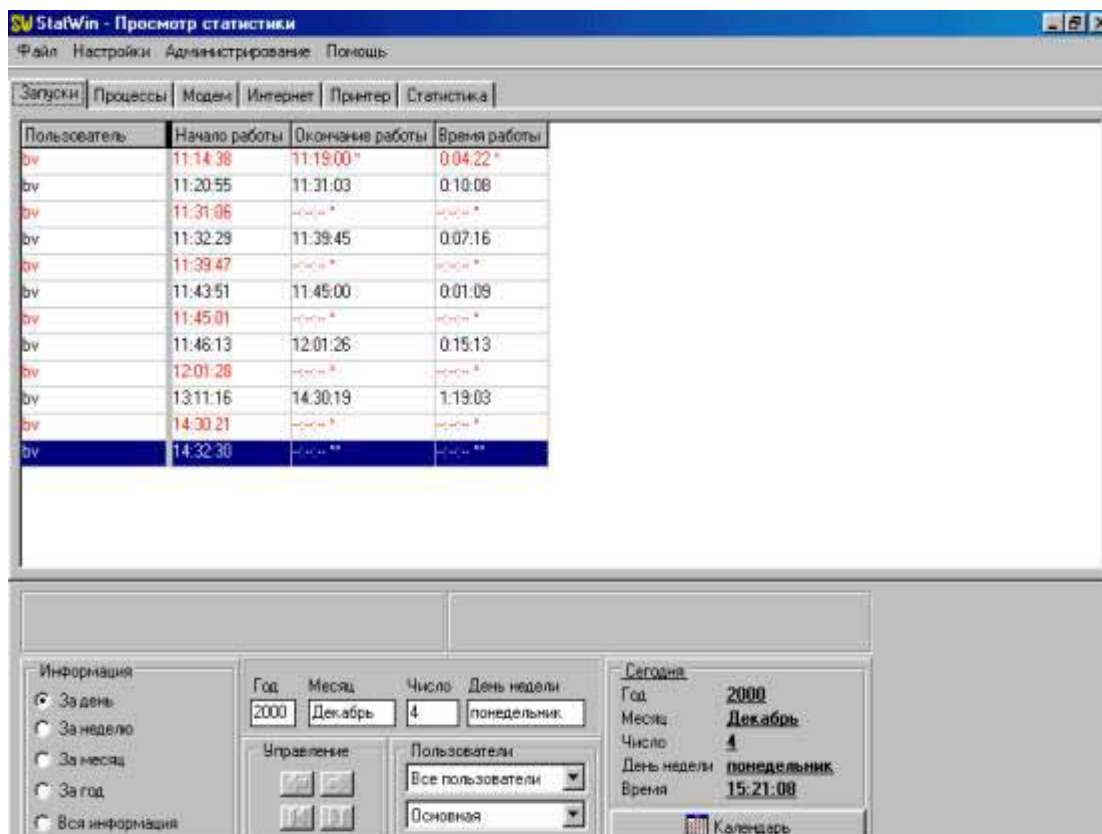


Рисунок. 1 Окно программы SeeStat

Программа выполняет следующие функции:

- Отмечает начало работы и конец работы на компьютере
- Log-in пользователя
- Учёт статистики (количество запусков, количество зависаний Windows, среднее время работы...)
- Контроль за процессами, исполняющимися в Windows.
- Контроль за работой в Интернет
- Контроль за работой принтера
- Позволяет просмотреть статистику за день, неделю, месяц, год или за весь период работы.

- Позволяет сохранить статистику в формате csv, что позволит в дальнейшем легко обрабатывать данную информацию с помощью программ управления базами данных

Как видно из основного окна программы мы можем просматривать запуски, процессы, отслеживать работу модема, работу с Интернет, принтером, статистику использования компьютера. С помощью программы можно запретить вход в Windows без пароля, что позволяет однозначно идентифицировать пользователя.

С помощью окна просмотра процессов можно определить, какие процессы и в какое время использовались (Рисунок 2).

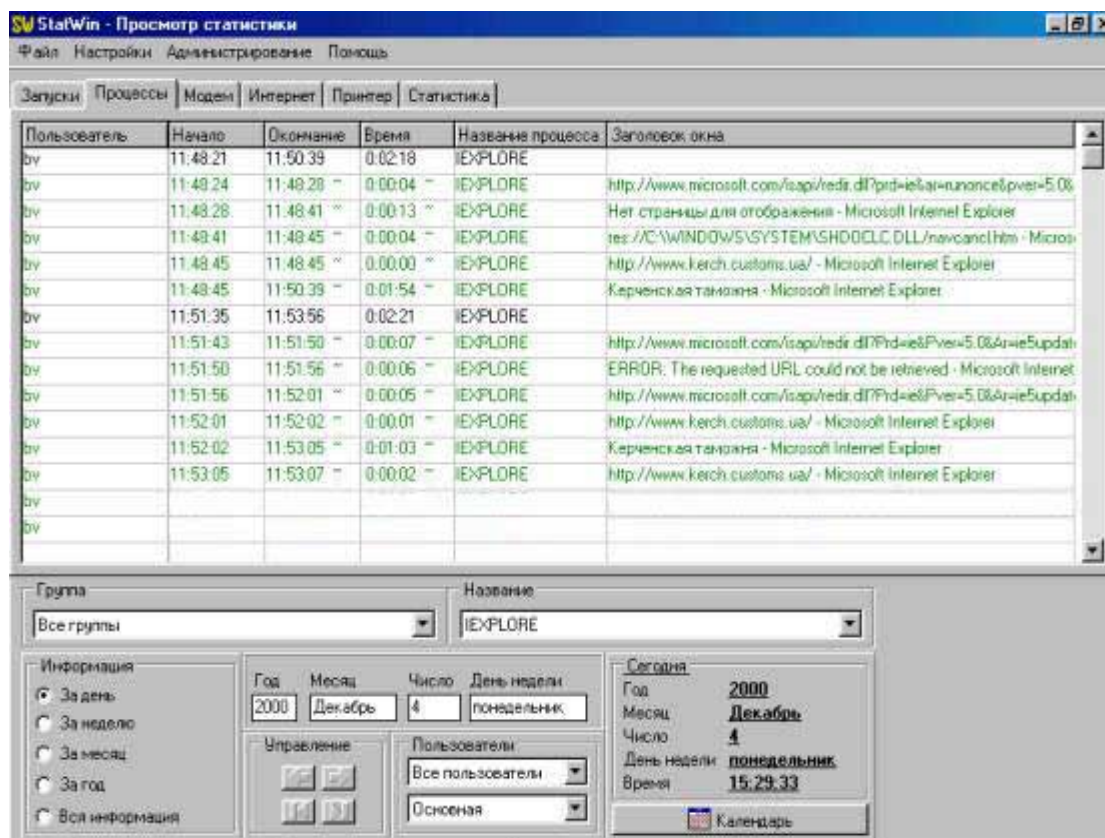


Рисунок 2 Окно процессов

При этом статистическая информация, собираемая на компьютере, может сохраняться и передаваться для дальнейшей обработки администратором на сервер сети локальной вычислительной сети, что упрощает ее анализ.

Для того чтобы скрыть программу от пользователя, применяется так называемый скрытый режим, при котором пользователь не видит выполнение данной программы. При нажатии Ctrl-Alt-Del в списке программ отсутствует программа ExecStat, то есть пользователь не знает о том, что все его действия протоколируются.

Достоинства

- Легко обрабатывает полученную информацию
- Разделяет ее по направлениям
- Позволяет управление списком отслеживаемых процессов.

Недостатки

- Программа видна в списке установленных программ.
- В случае работы компьютера под управлением Windows 98 при наборе в командной строке команды msconfig видна во вкладке Автозагрузка.

Invisible Activity Spy Config v2.3

Инсталляционный модуль занимает 405 kb. Программа состоит из модуля IasConfig.exe и ряда дополнительных библиотек и модулей.

Программа выполняет следующие функции:

- Отмечает начало работы и конец работы на компьютере
- Log-in пользователя
- Контроль запуска программ, исполняющихся в Windows.
- Контроль за работой в Интернет (наименование сайта, страницы)
- Контроль за работой принтера
- Контроль за работой буфера обмена (в файл протокола помещаются все данные, скопированные через буфер обмена)
- Шифрование файла протокола
- Пересылка файла протокола по e-mail.

На рисунке 3 представлено окно программы Invisible Activity Spy Config v2.3

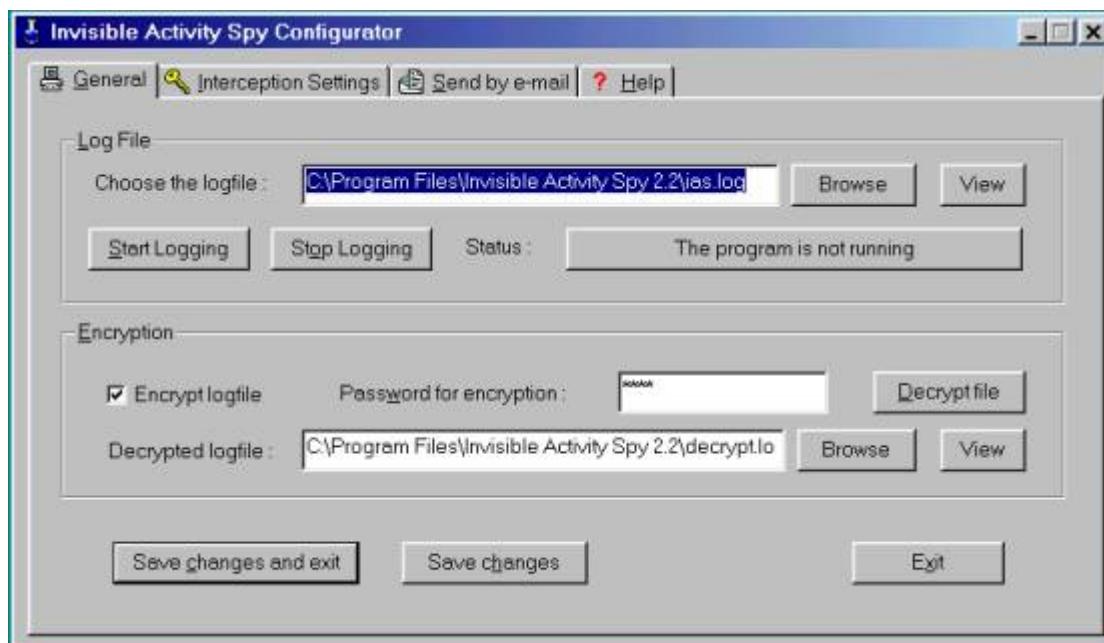


Рисунок 3 Invisible Activity Spy Config v2.3

С помощью окна установок параметров можно установить необходимые параметры работы программы. (Рисунок 4).

Достоинства

- Простота управления, легкость настройки.
- Контроль за работой буфера обмена (в файл протокола помещаются все данные, скопированные через буфер обмена)
- Шифрование файла протокола
- Пересылка файла протокола по e-mail.

Недостатки

- Программа видна в списке установленных программ.
- В случае работы компьютера под управлением Windows 98 при наборе в командной строке команды msconfig видна во вкладке Автозагрузка.
- Log-файл представляет из себя обычный текстовый файл, что затрудняет обработку.

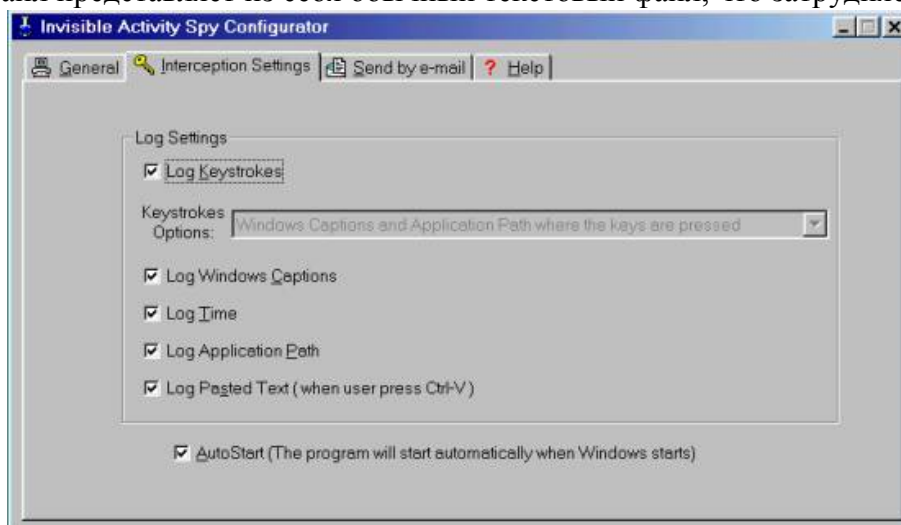


Рисунок 4 Установка параметров работы программы

Кроме вышеперечисленного программного обеспечения существует еще ПО, осуществляющее периодическое «фотографирование» экрана компьютера и создание текстовых файлов протоколов (в файл протокола помещаются все данные, скопированные через буфер обмена). Рассмотрим данный класс программного обеспечения на примере трех программ:

1. Inlook Express Control Panel (<http://www.Jungle-Monkey.com>)
2. PC Spy Present Softdd v2.31 (<http://www.softdd.com>)
3. Paparazzi Industar Cybernetics Corp. 1999-2000г. (<http://www.xakep.ru/post/10845/default.asp>)

asp)

Рассмотрим данный класс программного обеспечения более подробно

Inlook Express Control Panel

Программа состоит из единственного модуля inlook.exe, который при установке размещается в директории Windows. При этом программа не видна ни в списке установленных программ, ни при нажатии Ctrl-Alt-Del.

Предназначена для периодического «фотографирования» содержимого экрана, может применяться в виде «клавиатурного шпиона», так как позволяет отслеживать нажатия всех клавиш в промежутке между «фотографированиями» экрана. Позволяет шифровать log-файл. На рисунке 5 показано главное окно программы.

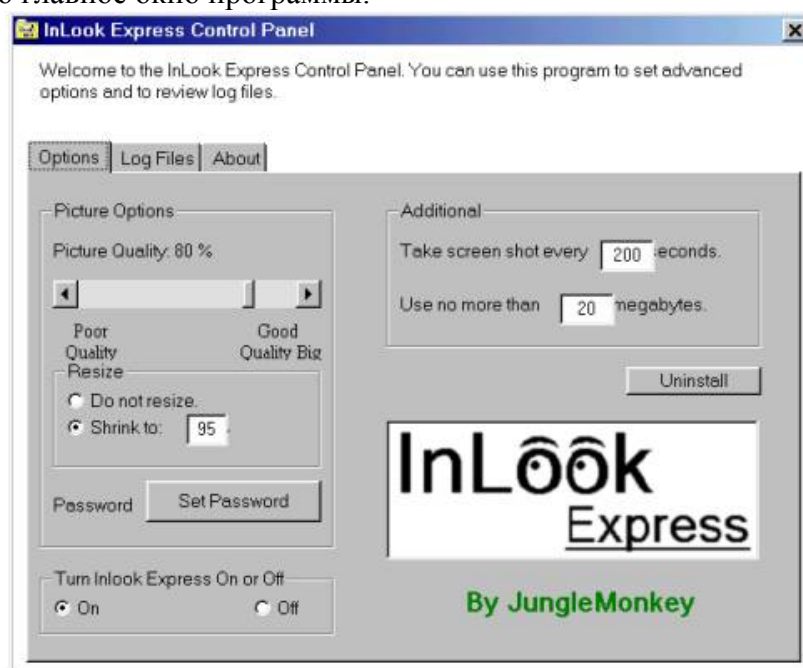


Рисунок 5 Главное окно программы

При работе программы периодически происходит «фотографирование» экрана и сохранение в специальном буфере всех значений нажатых клавиш в промежутке между фотографиями.

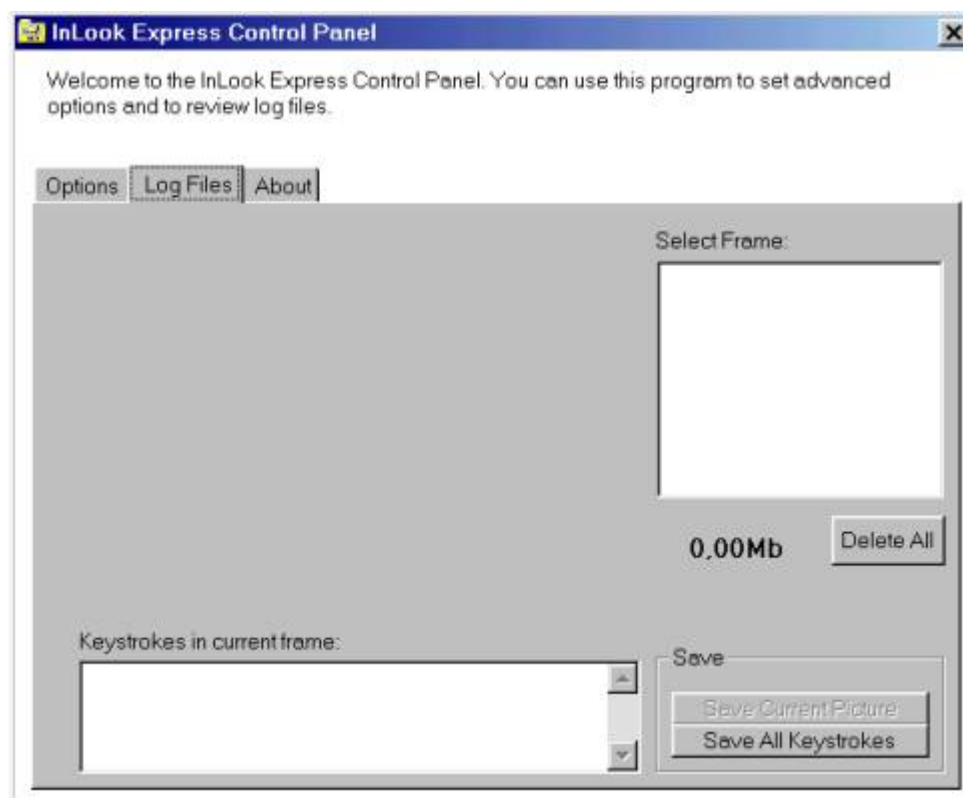


Рисунок 6 Окно файлов протоколов

Достоинства

- Не видно в перечне установленного программного обеспечения.
- Записывается непосредственно в каталог Windows, а поскольку состоит из всего одного файла, то это затрудняет обнаружение.
- Управление размером получаемых «фотографий».

Недостатки

- Большой объем сохраняемой информации
- Невозможность отследить, какому пользователю принадлежат «фотографии»
- Для получения результатов работы необходим физический доступ к компьютеру, на котором установлено данное программное обеспечение.

PC Spy Present Softdd v2.31

Программа состоит из единственного запускаемого модуля и библиотеки.

Как видно из Рисунка 7 данное программное обеспечение предназначено только для «фотографирования» экрана в процессе работы и может быть отнесено к классу «шпионов» персональных компьютеров.

Выполнение программы.

Вы можете включать эту программу в любое время, и она выполнится полностью невидимо. PC Spy не будет показано в перечне выполняемых задач, если пользователь нажимает CTRL-ALT-DEL (Win 95/98). Захваченные экраны не могут быть просмотрены любым нормальным средством просмотра графических файлов, но PC Spy может рассматривать их, используя "Перечень зарегистрированных изображений". Программа остановится автоматически, как только достигнет числа изображений, выбранного вами. Вы выбираете, как часто фиксировать отображаемые изображения (например, каждые 120 секунд) и число «фотографируемых» экранов перед остановкой. Как только PC Spy сохранил число экранов, которые Вы выбрали, он автоматически выключается. Вы можете также изменять норму сжатия для каждого сохраненного экрана. Это позволяет использовать намного меньшее количество дискового пространства для каждого изображения. Вы можете выполнять и возобновлять PC Spy с дискеты, затем вынуть дискету. Когда Вы желаете рассмотреть захваченные экраны, вставьте дискету, и запустите PC Spy, затем рассмотрите изображения, использующие "Зарегистрированные Изображения". (Это предохранит от любого обнаружения программы на вашей машине).

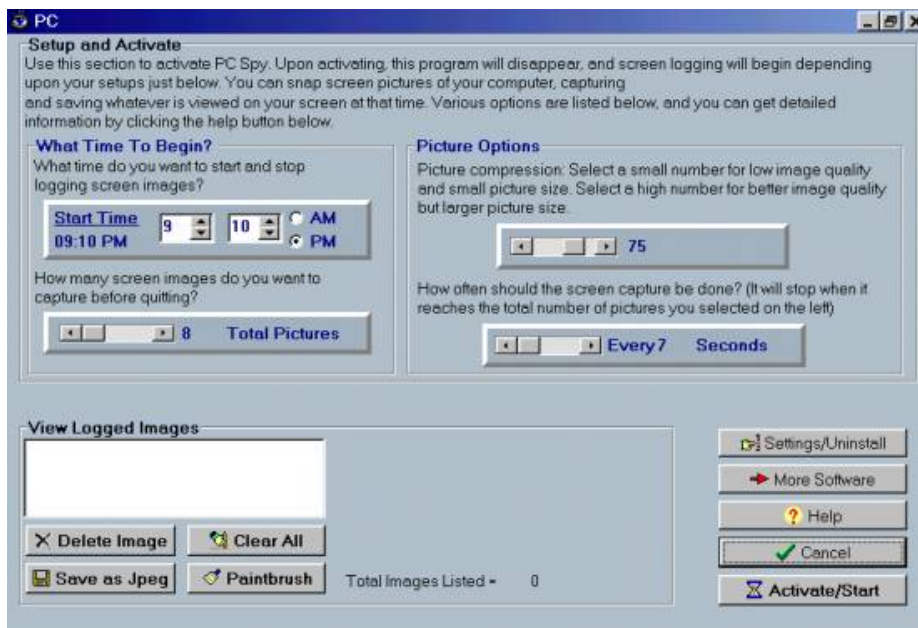


Рисунок 7 Главное окно программы PC Spy

Вы можете запускать программное обеспечение в любое время, но фактически «фотографирование» экрана начнется в указанное вами время.

Вы можете конвертировать и сохранять захваченные изображения, и Вы можете даже конвертировать их в изображения JPEG.

Недостатками данного программного обеспечения являются:

- Большой объем сохраняемой информации
- Невозможность отследить, какому пользователю принадлежат «фотографии»
- Для получения результатов работы необходим физический доступ к компьютеру, на котором установлено данное программное обеспечение.

Paparazzi Industar Cybernetics Corp. 1999-2000 г.

Комплект PAPARAZZI - это два независимо работающих модуля - "агент", который делает снимки и "клиент".

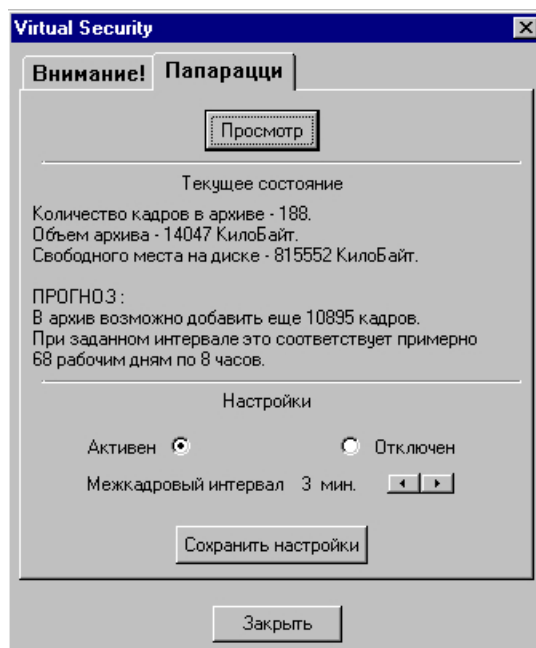


Рисунок 8 окно настройки модуля Paparazzi

Модуль "агент" устанавливается (устанавливается) на компьютер и скрытно работает на нем до удаления (деинсталляции), а "клиент" запускается с CD-ROMа каждый раз, когда нужно

просмотреть накопившиеся данные или изменить настройки PAPARAZZI - частоту кадров, удалить или сортировать снимки, приостановить наблюдение на любое время.

Программа использует методику защиты от контрнаблюдения, несанкционированного использования или случайного запуска. Файлы данных тщательно защищены от обнаружения и просмотра. Для пользования PAPARAZZI нужно помнить (и сохранять в тайне) пароль и код доступа. Не зная их, воспользоваться программой или просмотреть снимки просто невозможно.

В поле «Текущее состояние» отражается статистика работы программы и прогноз доступности ресурсов компьютера программе.

Настройте нужный вам интервал следования кадров (от 1 до 9 минут). Начальная установка программы – 3 минуты. Можете приостановить работу программы кнопкой «Активен-Отключен» Ваши настройки вступят в силу после нажатия кнопки «Сохранить настройки» Кнопка «Заккрыть» закрывает панель управления и возобновляет работу с текущими настройками.

Для просмотра накопленной информации открывается специальное окно монитора (рисунок 9) В заголовке окна монитора указано время и дата, когда был сделан кадр, количество сделанных кадров всего и порядковый номер текущего среди них.

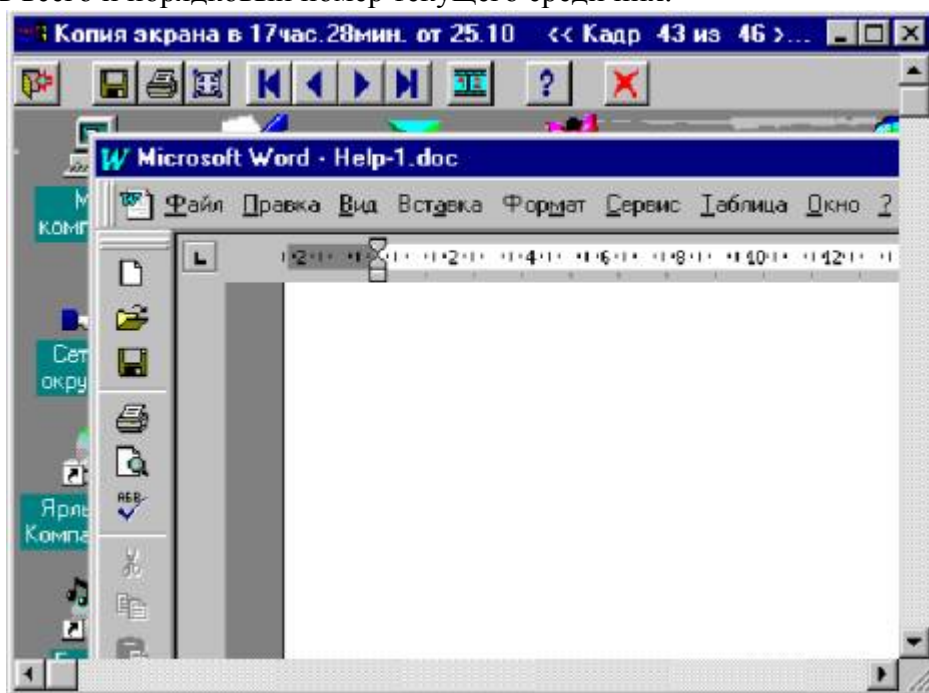


Рисунок 9 окно монитора Paparazzi

Кнопки панели монитора позволяют:

- записать выбранный кадр на дискету
- отпечатать кадр
- изменить масштаб показа
- промотать кадры к началу
- перейти к предыдущему кадру
- перейти к следующему кадру
- промотать кадры в конец
- просмотреть кадры как фильм
- просмотреть вспомогательные инструкции
- удалить просмотренное

Достоинства

- Легкость в настройке
- Невозможность обнаружения

Недостатки

- Большой объем сохраняемой информации
- Невозможность отследить, какому пользователю принадлежат «фотографии»

- Для получения результатов работы необходим физический доступ к компьютеру, на котором установлено данное программное обеспечение.

Серверная часть программного обеспечения

Серверной частью управляет только администратор безопасности вычислительной системы, т.к. информация, накапливаемая в журнале регистрации, при достижении определенного объема становится критичной, т.е. ее потеря или неправильное использование (модификация, ознакомление) может нанести ущерб владельцу информации или АС, или любому другому физическому (юридическому) лицу или группе лиц. Главная функция серверной части - централизованный сбор и хранение журналов регистрации, передаваемых от клиентских частей. Под журналом регистрации понимается упорядоченная совокупность регистрационных записей, каждая из которых заносится клиентской частью по факту совершения контролируемого события.

Наибольшая проблема при разработке серверной части - обеспечить устойчивую работу системы в том случае, когда серверная часть будет обслуживать десятки тысяч клиентов. При этом необходимо следить, чтобы не возникало "утечек" памяти из-за неполного освобождения объемов динамической памяти. Программы, реализующие свойство наблюдаемости ВС, - это очень сложные и дорогостоящие комплексы. Поэтому они должны обладать соответствующими мерами защиты от несанкционированного использования. Во-первых, применяются программные технологии защиты - проверка целостности кода и данных, шифрование данных, шифрование трафика между клиентскими и серверной частями и т.д. Во-вторых, применяются аппаратные ключи защиты, в которые прошивается персональная информация о заказчике, максимально допустимое количество клиентов, диапазон IP-адресов и др. Характерно, что программы наблюдаемости могут применяться не только в локальной сети предприятия, но и в глобальной сети Internet, поэтому необходимо жестко задавать диапазон IP-адресов клиентов и их максимальное количество, IP-адрес сервера и маску подсети.

Для удобного анализа журналов регистрации средствами систем управления базами данных (СУБД) необходимо предусмотреть возможность автоматического преобразования журналов регистрации в DBF- формат. Это позволяет применять SQL-запросы и делать выборки по интересующим критериям.

Выводы

Наиболее эффективную защиту автоматизированной системы обеспечивает только совокупность взаимосвязанных физических, технических и организационных мер. В современных условиях, особенно, когда тысячи компьютеров, принадлежащих одной организации, рассредоточены территориально (в разных зданиях, городах, странах), невозможно говорить о безопасности инфраструктуры автоматизированной системы без обеспечения ее наблюдаемости. Перспективными направлениями развития программ наблюдаемости являются:

- разработка модулей для звукового и видео контроля вычислительных систем, резко увеличивающих информативность отчетной информации;
- разработка многоплатформенных клиентских и серверных частей;
- разработка модулей по оперативному уведомлению администратора безопасности о состоянии серверной части и о нарушениях установленной политики безопасности с использованием средств сотовой и пейджинговой связи.

Литература

Наблюдаемость вычислительных систем как неотъемлемая часть комплекса средств защиты в автоматизированных системах Д. В. Кудин

Общество с ограниченной ответственностью "АННА"[®]

Запорожский государственный технический университет (<http://www.bezpeka.com>)

<http://bezopasno.narod.ru/p6.html>

ПРОГРАММНО-АППАРАТНЫМ МЕТОДАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ СВЯЗИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ОТНОСЯТСЯ:

- аппаратные шифраторы сетевого трафика;

- методика Firewall, реализуемая на базе программно-аппаратных средств;
- защищенные сетевые криптопротоколы;
- программно-аппаратные анализаторы сетевого трафика;
- защищенные сетевые ОС.

Методика Firewall как основное программно-аппаратное средство осуществления сетевой политики безопасности в выделенном сегменте IP-сети. В общем случае методика Firewall реализует следующие основные три функции:

1. **Многоуровневая фильтрация сетевого трафика.** Фильтрация обычно осуществляется на трех уровнях OSI:

- сетевом (IP);
- транспортном (TCP, UDP);
- прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация сетевого трафика является основной функцией систем Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику безопасности в выделенном сегменте IP-сети, то есть, настроив соответствующим образом Firewall, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящимся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Можно провести аналогию с администратором локальной ОС, который для осуществления политики безопасности в системе назначает необходимым образом соответствующие отношения между субъектами (пользователями) и объектами системы (файлами, например), что позволяет разграничить доступ субъектов системы к ее объектам в соответствии с заданными администратором правами доступа. Те же рассуждения применимы к Firewall-фильтрации: в качестве субъектов взаимодействия будут выступать IP-адреса хостов пользователей, а в качестве объектов, доступ к которым необходимо разграничить, - IP-адреса хостов, используемые транспортные протоколы и службы предоставления удаленного доступа.

2. **Проху-схема с дополнительной идентификацией и аутентификацией пользователей на Firewall-хосте.** Проху-схема позволяет, во-первых, при доступе к защищенному Firewall сегменту сети осуществить на нем дополнительную идентификацию и аутентификацию удаленного пользователя и, во-вторых, является основой для создания частных сетей с виртуальными IP-адресами. Смысл проху-схемы состоит в создании соединения с конечным адресатом через промежуточный проху-сервер (проху от англ. полномочный) на хосте Firewall. На этом проху-сервере и может осуществляться дополнительная идентификация абонента.

3. **Создание частных сетей (Private Virtual Network - PVN) с "виртуальными" IP-адресами (NAT - Network Address Translation).** В том случае, если администратор безопасности сети считает целесообразным скрыть истинную топологию своей внутренней IP-сети, то ему можно порекомендовать использовать системы Firewall для создания частной сети (PVN-сеть). Хостам в PVN-сети назначаются любые "виртуальные" IP-адреса. Для адресации во внешнюю сеть (через Firewall) необходимо либо использование на хосте Firewall описанных выше проху-серверов, либо применение специальных систем роутинга (маршрутизации), только через которые и возможна внешняя адресация. Это происходит из-за того, что используемый во внутренней PVN-сети виртуальный IP-адрес, очевидно, не пригоден для внешней адресации (внешняя адресация - это адресация к абонентам, находящимся за пределами PVN-сети). Поэтому проху-сервер или средство роутинга должно осуществлять связь с абонентами из внешней сети со своего настоящего IP-адреса. Кстати, эта схема удобна в том случае, если вам для создания IP-сети выделили недостаточное количество IP-адресов (в стандарте IPv4 это случается сплошь и рядом, поэтому для создания полноценной IP-сети с использованием проху-схемы достаточно только одного выделенного IP-адреса для проху-сервера). [\(продолжение\)](#) [хостинг в украине](#)

<http://www.suritel.ru/cgi-bin/view.pl?cid=1187156006&ProdId=pr71001>

Программно-аппаратные средства защиты информации от НСД

Программно-аппаратные комплексы "Соболь" и "Росомаха"



ПАК "Соболь" (версия 3.0)

Программно-аппаратный комплекс "Соболь" – это средство защиты компьютера от несанкционированного доступа, обеспечивающее доверенную загрузку.

ПАК "Соболь" обеспечивает контроль и регистрацию доступа пользователей к компьютерам, осуществляет контроль целостности программной среды и доверенную загрузку установленных операционных систем.

ПАК "Соболь" версия 3.0 сертифицирован ФСБ РФ (сертификат № СФ/027–1450 от 01.04.2010) и ФСТЭК России (сертификат № 1967 от 07.12.2009, переоформлен 11.03.2010), что позволяет использовать «Соболь» для защиты информации, составляющей коммерческую или государственную тайну в автоматизированных системах с классом защищенности до 1Б включительно.

Назначение:

ПАК «Соболь» может быть использован для того, чтобы:

- Доступ к информации на компьютере получили только те сотрудники, которые имеют на это право.
- В случае повреждения ОС или важных информационных массивов, хранящихся на компьютере, администратор мог вовремя принять меры по восстановлению информации.

Основные возможности:

• Аутентификация пользователей.

• Идентификация и усиленная (двухфакторная) аутентификация пользователей с использованием персональных идентификаторов. В качестве персональных идентификаторов пользователей могут применяться:

- - iButton
- - eToken PRO
- - iKey 2032
- - Rutoken S
- - Rutoken RF S

• Блокировка загрузки ОС со съёмных носителей.

• - После успешной загрузки штатной копии ОС доступ к этим устройствам восстанавливается.

• - Запрет распространяется на всех пользователей компьютера, за исключением администратора.

• Контроль целостности функционирует под управлением операционных систем, использующих следующие файловые системы: NTFS5, NTFS, FAT32, FAT16 и FAT12.

• Администратор имеет возможность задать режим работы электронного замка, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов.

• Электронный замок «Соболь» обеспечивает запрет загрузки операционной системы со съёмных носителей на аппаратном уровне для всех пользователей компьютера, кроме администратора.

• Контроль целостности.

- Используемый в комплексе "Соболь" механизм контроля целостности позволяет контролировать неизменность файлов и физических секторов жесткого диска до загрузки операционной системы.

- - Для этого вычисляются некоторые контрольные значения проверяемых объектов и сравниваются с ранее рассчитанными для каждого из этих объектов эталонными значениями.

- - Формирование списка подлежащих контролю объектов с указанием пути к каждому контролируемому файлу и координат каждого контролируемого сектора производится с помощью программы управления шаблонами контроля целостности.

- **Сторожевой таймер.**

- Механизм сторожевого таймера обеспечивает блокировку доступа к компьютеру при условии, что после включения компьютера и по истечении заданного интервала времени управление не передано расширению BIOS комплекса "Соболь".

- **Регистрация попыток доступа к ПЭВМ.**

- ПАК «Соболь» осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти. Таким образом, электронный замок «Соболь» предоставляет администратору информацию обо всех попытках доступа к ПЭВМ. В системном журнале фиксируются следующие события:

- - факт входа пользователя и имя пользователя;
- - предъявление незарегистрированного идентификатора пользователя;
- - введение неправильного пароля;
- - превышение числа попыток входа в систему;
- - число и дата НСД.

- **Поддержка платы PCI-Express.**

Достоинства ПАК "Соболь":

- Наличие сертификатов ФСБ и ФСТЭК России;
- Защита информации, составляющей государственную тайну;
- Помощь в построении прикладных криптографических приложений;
- Простота в установке, настройке и эксплуатации;
- Поддержка 64х битных операционных систем Windows;
- Поддержка идентификаторов iKey 2032, eToken PRO и Rutoken v.2.0.

Преимущества ПАК "Соболь":

- соответствие законодательным требованиям;
- защита от угроз связанных с получением доступа к компонентам ИСПДн (разграничение доступа, запрет загрузки с внешних носителей и т.д.);
- обеспечивает защиту от НСД и защиту персональных данных;
- соответствие условиям эксплуатации, прописанным в формулярах на продукты Secret Net, "Континент-АП", "КриптоПро CSP", СКЗИ М506А-2000 и М506А-XP.

Технические характеристики

Совместимость с ОС:

Windows Server 2008 / Server 2008 x64 Edition

Windows Vista (Enterprise, Business, Ultimate) / Vista Business x64 Edition

Windows Server 2003 / Server 2003 x64 Edition / Server 2003 R2 / Server 2003 R2 x64 Edition

Windows XP Professional / XP Professional x64 Edition

Windows 2000 / 2000 Server

FreeBSD версии 5.3, 6.2, 6.3 или 7.2

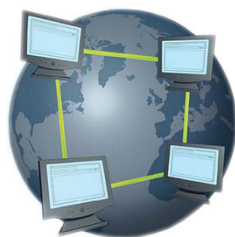
Trustverse Linux XP Desktop 2008 Secure Edition

MCBC 3.0

Юлия Шуткина, Александр Вирц

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРОВ

Для «взлома» требовался непосредственный контакт злоумышленника с машиной, вредоносные программы передавались только на сменных носителях, что не способствовало их массовому распространению и повальным эпидемиям. Главным источником угрозы стало появление и повсеместное использование сетевого доступа и всемирной сети Интернет.



Сетевой доступ и всемирная сеть Интернет – главный источник угроз ИПД

Широкое развитие локальные сети и Интернет получили к 1993 году. В это время в больших корпорациях начала распространяться практика создания локальных сетей для совместной работы с данными, а всемирная паутина стала с огромной скоростью плестись между многочисленными пользователями ПК. За короткое время несколько миллионов пользователей операционных систем Windows 95 и Windows 98 влились в Интернет, при этом абсолютно не подозревая о том, что это небезопасно для их компьютера.

Все знают: чем масштабнее сеть и чем ценнее информация, к которой имеют доступ подключенные пользователи, тем больше появляется желающих нарушить нормальное функционирование этой сети. Чаще всего ради выгоды, но порой и «от нечего делать». Вирусы, трояны, программы-шпионы со временем становились все сложнее и «умнее», методы внедрения вредоносного кода – все изощреннее. С другой стороны, появлялись все более интеллектуальные методы программного обнаружения зловредных программ, совершенствовались средства защиты информации на персональных компьютерах. И эта своеобразная «война» между пользователями и взломщиками длится уже много лет.



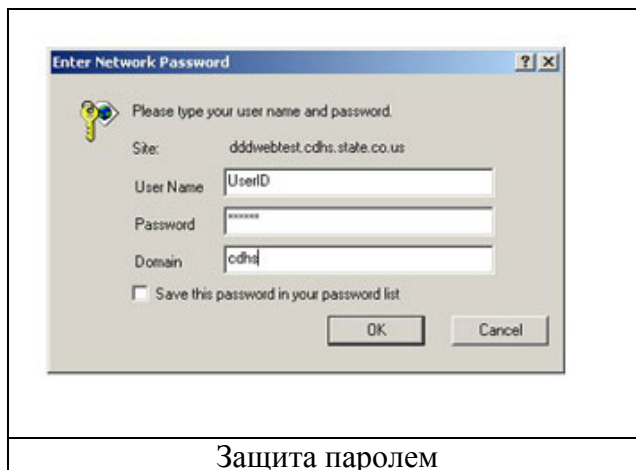
С тех пор прогресс шагнул далеко вперед, и на сегодняшний день существует большое количество способов обеспечения безопасности компьютера, некоторые из которых стали просто обязательной нормой поведения при работе с ПК. Причем это касается не только пользователей корпоративных сетей, но и обычных домашних «юзеров», компьютер которых оснащен невероятно популярным сегодня выходом в Интернет.

Идентификация пользователя

Защита паролем

Главным защитным рубежом по праву считается **система парольной защиты**. Каждый раз после включения компьютера работа с операционной системой начинается с элементарного

«знакомства»: мы сообщаем свое имя и пароль. Имя необходимо для идентификации пользователя, пароль в свою очередь подтверждает правильность произведенной идентификации. Введенная в диалоговом режиме информация сравнивается с той, которая находится в распоряжении операционной системы. Если они совпадают, пользователь получает доступ ко всем операциям, с которыми связано его имя. И как бы ни хотелось ускорить загрузку операционной системы, это средство защиты обязательно для всех пользователей сети, как корпоративной, так и домашней.



Самый распространенный способ взлома такого пароля – использование **парольного взломщика**. Как он работает? Атаке подвергается именно тот системный файл, в котором содержится информация о легальных пользователях и их паролях. Существующие на сегодняшний день операционные системы довольно хорошо защищают пользовательские пароли при помощи шифрования. Тем не менее, иногда «враг» путем различных ухищрений и лазеек все же пробивается к искомому файлу. Далее файл расшифровывается при помощи банального перебора ключей.

Какие действия нужно выполнить, чтоб ограничить злоумышленникам «простор для действий»?

1. Как уже упоминалось, стоит в обязательном порядке **устанавливать пароль на вход** в систему. И чем он будет сложнее (комбинации из латинских строчных и прописных букв, цифр и спецсимволов), тем больше времени у злоумышленника уйдет на его подбор

2. **Отключить загрузку** компьютера с компакт-дисков и сменных носителей

3. **Поставить пароль в BIOS** на включение компьютера и изменение его настроек

4. **Системный раздел** жесткого диска должен быть **в формате NTFS**. Именно эта файловая система на сегодняшний день обеспечивает максимальную сохранность и возможность шифрования личной информации

5. Следите за местонахождением **дисков аварийного восстановления и архивных копий**

Защита паролем – это, конечно, хорошо, но недостаточно надежно. Надежным способом защиты считается **многофакторная аутентификация**. Например, пользователь обязан предоставить смарт-карту или USB-ключ и ввести пароль. Этот вид защиты хорош тем, что «враг» не сможет ограничиться только взломом пароля. Чтобы получить доступ к вашему компьютеру, ему необходимо будет физическое устройство (ключ или смарт-карта). Эти устройства следует обязательно извлекать из компьютера по окончании работы.

Смарт-карты

Современные **смарт-карты** давно вытеснили своих предков – карты с магнитной полосой. Это не удивительно, ведь преимущества смарт-карт неоспоримы. Взять хотя бы их информационную емкость. Объем памяти смарт-карты в разы превышает емкость памяти карт предыдущего поколения. Смарт-карта долговечна и имеет очень высокую степень защиты данных от считывания и подделки.



Смарт-карта

Смарт-карта является безопасной при совместной работе защитных механизмов ее корпуса, операционной системы, чипа и приложения. Если же из строя выйдет хоть один из перечисленных компонентов, гарантия безопасности, увы, минимальна.

Существуют следующие виды так называемых «атак» на смарт-карты:

1. Социальные (атаки на людей, которые работают со смарт-картами). Чаще всего это банальное подглядывание при введении пин-кода.

2. Логические (действуют за счет криптоанализа и «троянских коней» в исполняемом коде смарт-карты). Эти атаки, пожалуй, самые успешные из всех существующих на данный момент.

Для защиты от этих атак достаточно не предоставлять смарт-карту посторонним людям и предусмотреть какие-либо средства от подглядывания кода, например, непрозрачные экраны, расположенные по обе стороны от клавиатуры.

USB-ключ

Принцип работы USB-ключа заключается в следующем: после инсталляции специальной программы компьютер не включится до тех пор, пока USB-ключ не будет вставлен в специальный порт. Порой сам ключ выступает как носитель информации небольшого объема, в памяти которого, кстати, можно хранить свой пароль



USB-ключ

Использование USB-ключа дает пользователю ряд преимуществ.

Во-первых, используется **более сложный пароль**, который автоматически передается в систему.

Во-вторых, больше **не надо отвлекаться на пароли**, если нужно на некоторое время отойти от компьютера. Вытащите ключ, и ПК заблокируется автоматически. По возвращении просто вставьте ключ на место.

В-третьих, можно использовать **один USB-ключ для доступа** к рабочему и домашнему компьютеру.

И, наконец, один из самых важных моментов – ключ практически **невозможно подделать**.

TPM-модули

Разработчики этого устройства нашли самый безопасный способ защиты – идентификация пользователя должна производиться еще до запуска операционной системы. Основная идея TPM-модуля состоит в аппаратной криптографической защите цифрового контента и проверке ваших прав на его использование. Проще говоря – никто, кроме владельца компьютера, не

сможет им воспользоваться. Также не помогут всевозможные ухищрения наподобие использования жесткого диска в другом компьютере, так как вся информация зашифрована, и ключ для расшифровки жестко привязан к аппаратной части компьютера. Устройство представляет собой микросхему или PCI-адаптер, установленные в материнскую плату компьютера.

Решения для безопасной работы в сети

Если с защитой от непосредственного контакта мошенника с компьютером мы разобрались, то как защититься от злоумышленника, пытающегося навредить удаленно, по сети? Следует сразу заметить, что в большинстве случаев пользователь сам по незнанию или беспечности «помогает» таким вредителям.



Ниже представлен список рекомендаций, которые помогут обеспечить безопасность компьютера и усложнить труд «возможного противника»:

- Удостоверьтесь, что ваше **решение безопасности (антивирус, файервол) активно и обновлено**. Необходимо, чтобы ваш антивирус работал не только на поиск известных и уже занесенных в базу данных вредоносных кодов, но и был обеспечен проактивной технологией поиска неизвестных угроз. Хорошо, если ваше антивирусное решение дополнительно оснащено брандмауэром.

- Особое внимание уделите электронной почте, так как именно она чаще всего является источником угроз, включая фишинг и розыгрыши, рассылаемые со спамом. **Игнорируйте любые запросы на предоставление персональной информации**, даже если они рассылаются якобы от имени Вашего банка, а также любые массово рассылаемые «заманчивые» предложения. Убедитесь, что ваш антивирус настроен на сканирование всей входящей и всей исходящей почты. Игнорируйте сообщения, поступающие от неизвестных отправителей.

- Внимательно **следите за появлением обновлений к программному обеспечению** и скачивайте их без промедления. Для атаки кибер-преступники часто пользуются «дырами» в системе безопасности популярных программ. Создатели в таких случаях обычно разрабатывают средства защиты для ликвидации обнаруженных уязвимостей. Если приложения автоматически не извещают о возможности скачивания новых версий, посетите веб-страницу разработчиков - там можно узнать о наличии доступных обновлений.



- Старайтесь **не загружать программы с сомнительных сайтов**, потому что существует угроза заражения. Это также касается загрузок в P2P сетях. Многие угрозы маскируются под файлы с заманчивыми названиями, чтобы привлечь пользователей, заставить их скачать файл и запустить на своем компьютере.



- **Отклоняйте любые неизвестные вам файлы**, присылаемые из чатов и групп новостей: они могут содержать вредоносные коды.

- **Никогда не сообщайте конфиденциальных сведений о себе** людям, с которыми только что познакомились в чате, IRC и т.д. Еще неизвестно, что за человек находится по другую сторону. Поэтому старайтесь не выдавать сведений, которые способствовали бы установлению вашего местонахождения.

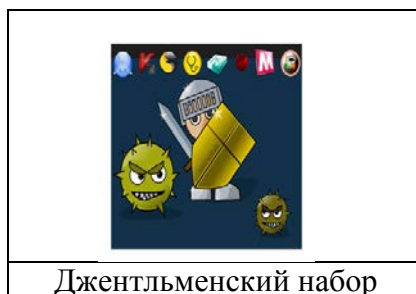
- **Делайте покупки только в хорошо зарекомендовавших себя интернет-магазинах** и никогда ничего не покупайте на сайтах, где транзакция выполняется не по протоколу безопасности и без шифрования информации. Определить, защищена ли веб-страница, можно по наличию сертификата безопасности – иконки в виде желтого замочка в командной строке браузера или в правой нижней части экрана.

- **Не используйте общественные компьютеры** для проведения транзакций, которые требуют от вас введения паролей или личных данных.

- **Используйте программы родительского контроля.** Летом дети чаще пользуются компьютером. Важно научить их ответственному отношению к использованию интернета, определить возможное время, проводимое детьми за компьютером, присматривать за ними и ограничить доступ к определенным страницам и любому недопустимому контенту.

Джентльменский набор

Для наиболее полноценной защиты личных данных и обеспечения безопасности компьютера в сети на нем должен быть обязательно установлен «джентльменский набор» программ: антивирус, брандмауэр и антиспам.



Антивирус

Компьютерных вирусов сейчас великое множество, и любой известный антивирус «знаком» с большинством из них. По минимуму задача антивируса состоит в отслеживании действий, производимых программами над жизненно важными элементами операционной системы

и данными. Так что если на компьютере установлен антивирус, минимальная защита компьютеру обеспечена.

Но не стоит надеяться, что антивирус, отражая большинство вредоносных программ, не пропустит ту, которая ему неизвестна. Поэтому регулярно, по первому требованию самой программы, обновляйте вирусные базы данных! Ведь в этом и состоит основной плюс антивирусов – быстрое реагирование на появление новой угрозы до того, как она успела распространиться повсеместно.

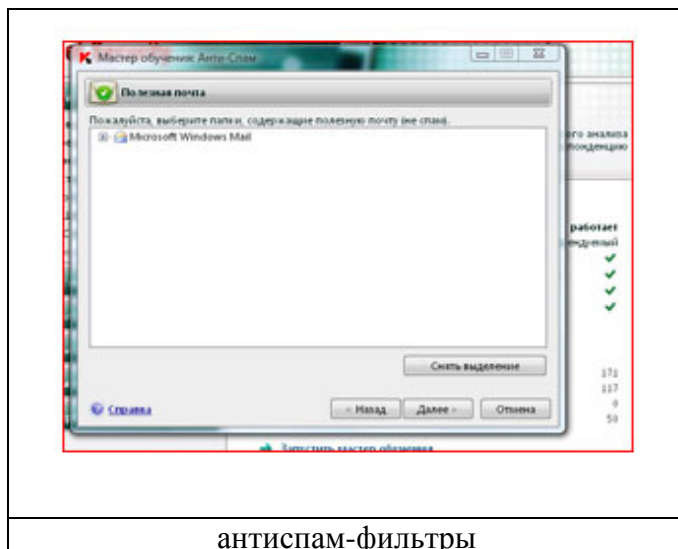
Среди этих защитников существуют, кстати, и бесплатные варианты. Большая их часть является урезанной версией платного решения, но есть и вовсе оригинальные. Указав такой программе на подозрительный файл, можно загрузить его с вашего компьютера на специальный «санитарный» сервер, его проверит «серьезный» антивирус и выдаст результат. Разумеется, антивирус – это всегда хорошо. Но в некоторых случаях даже он не в силах помочь. Речь идет об удаленном доступе злоумышленника к ресурсам компьютера.

Файервол (брандмауэр)

Файервол (брандмауэр) – программа, ограничивающая несанкционированный доступ по двум направлениям: извне, со стороны программ или других пользователей, и изнутри, со стороны установленных программ, пытающихся без ведома пользователя передавать какие-либо данные в сеть.



Стандартным файерволом оборудованы все компьютеры, на которых установлена ОС Windows XP SP2 и выше. Этот полезный шаг разработчики операционной системы сделали в связи с возросшим уровнем активности злоумышленников, атакующих компьютеры пользователей через Интернет. Минус его в том, что он требует специальных настроек и обязательных знаний от пользователя. Не обладая этими знаниями, пользователь простым нажатием кнопки «ОК» во всплывающих окнах может легко свести на нет защиту своего компьютера.



Более серьезные и специализированные решения намного лучше защищают компьютер от злоумышленников, но в настройках большинства из них способен заблудиться даже продвинутый пользователь. Для более «плавного» знакомства с функционалом подобных программ в них стали предусматривать «режимы обучения» с подробной справкой. Пользователь, создавая правила, разрешающие или запрещающие доступ к сети со стороны программ, сам начинает понимать значение своих действий, попутно возводя поистине индивидуальную защиту. Для тех, кому лень хоть немного разбираться с настройками, существуют предустановленные варианты защиты (light, medium, lager J). Ну и, конечно, стандартные «запретить все» и «разрешить все», оставленные не для практического использования, а скорее для тестирования настроек.

В паре с программой-антивирусом, фаервол образует достаточно мощный заслон от опасностей виртуального мира.

Антиспам

Все мы слышали о правилах безопасности при пользовании интернетом. Одно из самых главных - ни в коем случае не открывать письма, присланные на ваш электронный адрес незнакомым человеком. Чтобы исключить возможность любого «спама», существуют специальные **антиспам-фильтры**.

Принцип их работы следующий: письма, приходящие на вашу почту, отфильтровываются с помощью специальных списков стоп-слов, встречающихся в теле письма, и огромной базы адресов известных спам-серверов. Вся сомнительная корреспонденция по желанию может либо сразу уничтожаться, либо помещаться в специальную папку на карантин. Чаще предпочтителен второй вариант, чтобы иметь возможность восстановить нужное письмо, если оно не прошло «фейс-контроль».

Дырки в сетке

Итак, защититься в сети мы теперь сможем... Но как защитить саму сеть?

Сейчас уже никого не удивит наличием в доме или в офисе Wi-Fi сети. Беспроводные точки доступа по Wi-Fi (хот-споты) в крупных городах порой перекрывают друг друга почти полностью. Хорошим тоном стало наличие беспроводного доступа в кафе, ресторанах, гостиницах, учебных заведениях и других местах скопления людей. Само собой, встает вопрос о том, как защитить подобные сети от вторжения «непрощенных гостей», способных навредить пользователям или данным.

Обезопасить беспроводную сеть от несанкционированного вторжения можно только с помощью шифрования. Сейчас повсеместно используется новая **технология WPA**. Особенностью и одновременно преимуществом этого вида защиты является **шифрование данных с динамически изменяемыми ключами**, создаваемыми заново на время каждого сеанса связи. На сегодняшний день самыми надежными считаются устройства, поддерживающие стандарт **802.11i (WPA2)** – никому пока не удалось их взломать.



Wi-Fi оборудование

Сегодня вопрос безопасности компьютера касается не только профессионалов, каждый пользователь должен уделять этой проблеме серьезное внимание. Не стоит думать, что ваш

компьютер никому не нужен. Всегда найдутся люди, которым он понадобится, хотя бы для рассылки спама или вредоносного программного обеспечения от вашего имени.

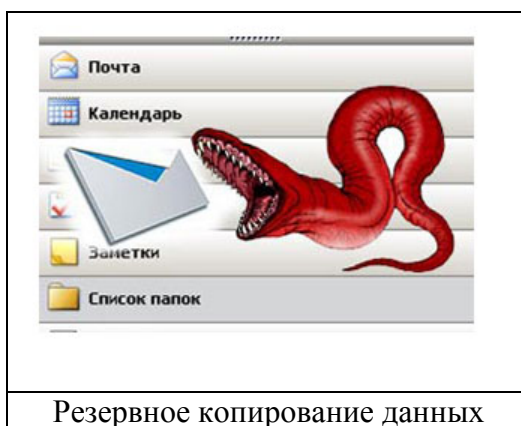
Организуя домашнюю беспроводную сеть, не пренебрегайте возможностями шифрования, уже изначально заложенными в Wi-Fi оборудование. Правила для составления статичных ключей такие же, как и для входа в операционную систему – чем длиннее и непонятнее будет набор символов, тем лучше. Длина ключа на скорость соединения не влияет, поэтому «не жалейте букафф»!

Возможность «подцепить» компьютерный вирус или троянскую программу на неизвестном сайте или из случайного электронного сообщения волей-неволей заставляет пользователей устанавливать и использовать антивирусы и сетевые экраны. Практически невозможно найти компьютер, где не было бы этих программ. Дополнительную напряженность нагнетают производители антивирусных утилит, рапортующие практически ежедневно о появлении новых опасностей.

Однако немногие задумываются о дальнейшей защите ценной информации, ограничиваясь антивирусом/файрволом, в то время как ни один из них не может предоставить полную гарантию сохранности важных данных.

Системы резервного копирования и восстановления данных

Между тем существует возможность обеспечить максимальную сохранность информации старым как мир способом – **резервным копированием данных**. Преимуществ у резервной копии несколько:



- Она никак **не связана с оригинальным источником** и программным обеспечением, за исключением программы-архиватора;

- Обычно **хранится в недоступном другим программам месте**, например на CD/DVD-диске;

- Содержит **точную копию оригинальных данных**, которая может быть легко извлечена и использована вместо поврежденных или утраченных данных;

Впрочем, как и любая технология, резервное копирование имеет свои недостатки:

- Для обеспечения сохранности архивных копий необходимо либо **выделение свободного дискового пространства** (которое могло быть использовано более рационально), либо **ручная работа с внешними носителями**;

- В некоторых случаях процесс создания резервной копии **сильно загружает компьютер** либо требует прекращения любой другой работы на нем;

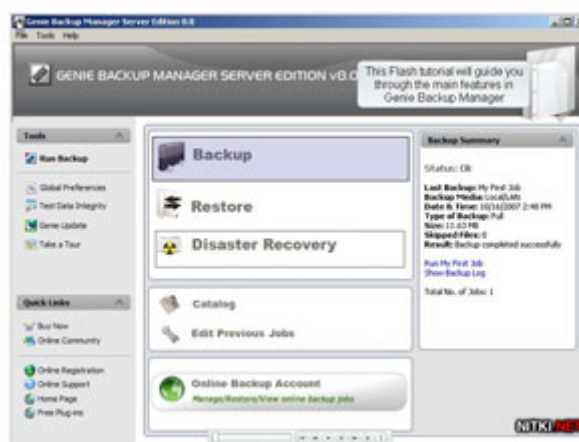
- Процесс восстановления данных **требует некоторого времени** и трудовых затрат;

- Восстановить информацию можно только в том случае, если она была предварительно сохранена. Изменения, внесенные после сохранения, могут оказаться **потерянными безвозвратно**.

Поскольку технология резервного копирования - ровесница самих персональных компьютеров, в ходе продолжительного совершенствования информационных технологий было выпущено большое количество различного программного обеспечения, цель которого - облегчить

создание архивных копий, управление ими и предоставить новые способы сохранения данных. Наиболее успешные из утилит превратились в программные комплексы, защищающие данные в масштабах от единичного компьютера до громадной сети и обладающие широкими функциональными возможностями. Например, одним из наиболее интересных вариантов использования подобных программ является **создание резервной копии операционной системы**.

После установки на компьютер «свежей» операционной системы, всех необходимых драйверов и программ нужно остановиться и сделать очень важную вещь - сохранить результат работы в виде системной резервной копии! В дальнейшем можно будет очень легко вернуться к первоначальному, стабильному состоянию операционной системы и компьютера. Фактически данная резервная копия будет служить гарантией, что больше никогда не придется восстанавливать все с нуля, а время простоя компьютера составит не часы или дни, а несколько минут, которые уйдут на поиск архива, загрузку с диска и распаковку данных. Сохранить архивы можно на особый защищенный раздел жесткого диска или прожечь на болванку.



Создания резервных копий

Стоит еще раз напомнить, что сохранность важной информации зависит от многих факторов и опирается на комплекс защитных мер, в котором программа создания резервных копий играет далеко не последнюю роль. При своевременном и постоянном использовании такая программа обеспечит надежное хранение операционной системы, файлов и папок пользователя, важных данных и ценной информации.

Как защитить ноутбук

Ноутбук за счет своей мобильности подвергается большему риску, чем стационарный ПК. Специфика пользования ноутбуком заставляет искать все новые и новые методы его защиты. Сейчас мы поговорим о, так сказать, «рейтинговых» способах защиты, проверенных массовым пользователем.

Замок Кенсингтона

Одно из самых простых и распространенных устройств, подходящее рядовому пользователю по качеству и цене. Если вы работаете с ноутбуком в офисе или на выездной презентации, но нужно срочно куда-либо отойти, замок Кенсингтона (Kensington Lock) - идеальный вариант защиты ноутбука от хищения. Как он действует? При помощи маленького металлического троса компьютер крепится к тяжелому стационарному предмету. Унести компьютер просто невозможно, единственный минус этого способа защиты - неудобство при переноске ноутбука, например, по комнате. Каждый раз трос нужно отсоединять.



Замок Кенсингтона

Сигнализация

Еще один вид защиты – сигнализация и все ее разновидности. Способов защиты на основе сигнализации множество, как и вариантов условий ее срабатывания. Например, она может сработать, если ноутбук куда-либо переместился или его удалили из определенной зоны.

Сканер отпечатков пальцев

В последнее время большую популярность приобрели биометрические сенсоры, или считыватели отпечатков пальцев. Это отличный способ защиты: отпечаток почти невозможно подделать или потерять, к тому же он всегда с вами.



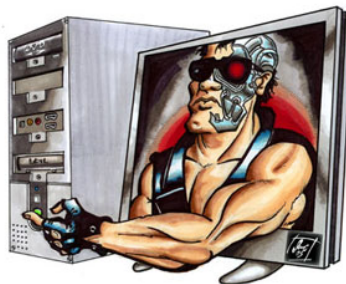
Биометрические сенсоры

Но, как и у прочих способов защиты, у биометрических сенсоров есть свои недостатки. Например, сенсор может просто не распознать отпечаток. Чтобы этого не произошло, можно снизить порог чувствительности устройства. Но, к сожалению, это приводит к снижению безопасности.

Для ноутбуков, не имеющих встроенного сканера отпечатков пальца, можно отдельно приобрести биометрический сканер, выполненный в виде обычной флешки. Помимо повышения безопасности данных, защищенных таким способом, данное решение обладает «побочным» преимуществом – вынув сканер из USB-порта, вы оставите с носом злодея, который за долгие зимние вечера сумел-таки подделать ваш отпечаток пальца.

Пишу из горящего танка...

Существует специальное программное обеспечение, которое, будучи установленным на компьютер, помогает найти ноутбук в случае его кражи. Работает оно так: как только похищенный ноутбук подключат к сети или он окажется в зоне действия беспроводных сетей, ПО сразу же сообщит о своем местонахождении в соответствующие организации.



На самом деле это не очень надежный вид защиты, так как подобное ПО устанавливается в большинстве случаев на уровне операционной системы. И если злодей, присвоивший себе ваш ноутбук, позже переустановит систему или полностью заменит жесткий диск, то шанс вернуть нажитое непосильным трудом становится призрачным. Специально для таких случаев было разработано программное обеспечение уровня BIOS, которое сообщает о своем местонахождении без привязки к операционной системе. Будем надеяться, что в дальнейшем подобным ПО будут комплектоваться все модели ноутбуков или его сделают обязательным для новых версий BIOS.

Заключение

Очень часто в нестабильной работе операционной системы мы виним ее разработчика, ссылаясь на его некомпетентность. Многие даже не подозревают о том, что эти проблемы возникают по нашей же вине.

Благодарим компании **Paragon Software** и **Panda Security** за помощь в подготовке материала

Источники:

www.paragon.ru
www.viruslab.ru

Контактная информация Проминформ - ЗАЩИТА ИНФОРМАЦИИ

• Россия, 614000, г. Пермь, ул. Газеты «Звезда», 24а +7 (342) 212-35-94; 212-93-87

- [О компании](#)
 - [Обращение директора](#)
 - [Лицензии](#)
 - [Вакансии](#)
 - [Менеджмент](#)
- [Новости](#)
- [Контактная информация](#)

[Партнеры](#)

Информация для клиентов

- [УСЛУГИ](#)
 - [Проектирование](#)
 - [Прокат оборудования](#)
- [ЗАЩИТА ИНФОРМАЦИИ](#)
 - [Защита персональных данных](#)
 - [Программные и программно-аппаратные комплексы защиты информации](#)
 - [Региональный центр специальных экспертиз](#)
 - [Отдел технической защиты информации](#)
 - [Аттестация объектов информатизации](#)
 - [Специальные исследования технических средств и систем](#)
 - [Специальная проверка и специальные обследования](#)
 - [Продажа спецтехники](#)
 - [Оказание услуг в области защиты Государственной тайны](#)
- [КАТАЛОГ ПРОДУКЦИИ](#)
 - [Аппаратно-программные комплексы для залов заседаний](#)
 - [Конференц-системы](#)
 - [Дискуссионная система СН-400](#)
 - [Состав оборудования](#)
 - [Варианты использования конференц-системы СН-400](#)
 - [Сравнительные характеристики дискуссионных конференц-систем](#)
 - [Цифровая конференц-система CSD-124](#)

- [Модуль управления](#)
- [Пульт делегата](#)
- [Пульт председателя](#)
- [ПЭВМ с блоком сопряжения](#)
- [Система аудио конференц-связи](#)
- [Система электронного голосования](#)
- [Общие сведения](#)
- [Модуль управления](#)
- [Оборудование рабочего места](#)
- [Пульт голосования](#)
- [Модуль индикации](#)
- [Варианты исполнения и внешний вид оборудования рабочих мест](#)
- [Система отображения результатов голосования](#)
- [Система регламентации времени выступлений](#)
- [Специальная техника](#)
- [Комплекс защиты FM-140](#)
- [Оборудование документирования устных выступлений](#)
- [Система синхронного документирования устной речи](#)
- [Компьютерные траскрайберы "Стенограф" и "Транскрайбер-SB"](#)
- [Многоканальная система записи, регистрации и архивирования звуковых сигналов](#)
- [Цезарь](#)
- [Оборудование синхронного перевода речи](#)
- [Проводная система перевода речи](#)
- [ИК-система перевода речи](#)
- [Системы звукоусиления](#)
- [Система MediaMatrix](#)
- [Общие сведения](#)
- [Основные достоинства MediaMatrix](#)
- [Принципы работы MediaMatrix](#)
- [Модели и системная поддержка](#)
- [X-FRAME](#)
- [X-FRAME-88](#)
- [Цифровые интерфейсы для центральных процессоров MediaMatrixT](#)
- [A/A-8P](#)
- [Центральные процессоры MediaMatrixT](#)
- [Программное обеспечение для аппаратно-программных комплексов MediaMatrixT](#)
- [Эквалайзеры](#)
- [Усилители мощности](#)
- [Микшерные пульта](#)
- [Автомикшеры](#)
- [Компрессор/лимиттер/гейт](#)
- [Акустические системы](#)
- [Источники аудио/видео сигнала](#)
- [Оборудование для мультимедиа презентаций](#)
- [Общее описание](#)
- [Мультимедиа-проекторы](#)
- [Экраны](#)
- [Визуалайзеры и презентеры](#)
- [Электронные копируемые блоки](#)
- [Интерактивные или сенсорные доски](#)
- [Сенсорные системы типа "антенна на поверхности"](#)
- [Интерактивные доски обратной проекции](#)
- [Интерактивные насадки на плазменные панели](#)
- [Оборудование технологического телевидения](#)
- [Технические данные и комплектность](#)
- [Типовая структурная схема конференц-системы](#)
- [Видеоконмутатор Panasonic](#)
- [Видеокамера Panasonic](#)
- [Пульт управления ПВ-03](#)
- [Прочее оборудование](#)
- [Блок раздачи для журналистов БРУ-055](#)
- [Блок трансформаторов](#)
- [Блок раздачи сигналов D-022](#)

- [Комплекс Обеспечения Проведения Заседаний 7-го поколения](#)
- [Аппаратно-программные комплексы для идентификации номеров автотранспортных средств](#)
- [Статистические данные](#)
- [Программное обеспечение](#)
- [Комплекс "СОВА-2"](#)
- [Технические характеристики](#)
- [Мобильный комплекс "СОВА-2М"](#)
- [Технические характеристики](#)
- [Многофункциональный контроллер для считывания номеров транспортных средств](#)
- [Прочее оборудование](#)
 - [Переговорные устройства серии УГС](#)
 - [Оборудование для системы оповещения](#)
- [ПРОЕКТЫ](#)
- [Аппаратно-программные комплексы для залов заседаний](#)
- [Аппаратно-программные комплексы для идентификации номеров автотранспортных средств](#)
- [Прочее оборудование](#)
- [ЗАКАЗ](#)
 - [Запрос информации](#)

Авторизация

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с Конвенцией Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (ETS №108, 1981г.) 27 июля 2006г. вступил в действие Федеральный закон от N 152-ФЗ "О персональных данных", согласно которому все информационные системы персональных данных (ИС ПД) компаний должны быть приведены в соответствие требованиям данного закона по защите персональных данных не позднее 1 января 2010 года. В сферу действия последнего попадают все государственные и муниципальные органы, юридические и физические лица, которые собирают, учитывают, обеспечивают хранение, администрирование, передачу и обработку персональных данных граждан РФ (сотрудников, клиентов, партнеров и т.п.).

В настоящее время установлены четыре категории персональных данных, отражающие их характер - от обезличенной и общедоступной персональной информации (четвертая категория) до сведений о расовой и национальной принадлежности, политических взглядах, религиозных убеждениях, состоянии здоровья и т.п. (первая категория). Как следствие, любая информационная система, обрабатывающая персональные данные, в зависимости от категории этих данных, их объема и степени детализации, распределенности информационной системы и ряда других факторов должна быть отнесена к определенному классу, а уровень ее защищенности - соответствовать критичности данных. Другими словами, к информационным системам разных классов предъявляются различные требования с точки зрения защиты персональных данных от несанкционированного доступа, уничтожения, изменения, копирования, распространения и иных неправомерных действий. Для некоторых классов информационных систем, обрабатывающих персональные данные, требуется развертывание нескольких средств информационной безопасности, включая подсистемы антивирусной защиты, анализа защищенности и выявления уязвимостей, криптографической защиты информации, маршрутизации, коммутации и межсетевого экранирования, обнаружения вторжений и даже защиты информации от утечки по техническим каналам. Существенно, что все средства защиты персональных данных должны быть сертифицированы ФСТЭК или ФСБ.

Мероприятия по обеспечению безопасности ПД осуществляются на основе законодательства Российской Федерации, нормативных и методических документов.

Проведение этих работ могут осуществлять только компании, обладающие необходимыми лицензиями!

Сегодня подавляющее большинство информационных систем хранят и обрабатывают такие сведения персонального характера, как фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия. По некото-

рым оценкам, на конец 2008г. в Российской Федерации насчитывалось от 4,5 до 7,5 миллионов операторов персональных данных, информационные системы которых должны быть защищены. Принятие закона «О персональных данных» привело к тому, что обеспечение безопасности персональных данных стало неотъемлемой частью эксплуатации информационных систем.

Хотя на приведение информационных систем в соответствие с положениями закона у операторов персональных данных остались считанные месяцы, опросы представителей российских компаний указывают на то, что многие организации до сих пор даже не инициировали соответствующие проекты. Среди причин такого положения дел следует назвать сравнительно позднее появление полного набора нормативных актов, относящихся к данной сфере, сложности с финансированием соответствующих проектов, неготовность к модернизации бизнес-процессов, затрагивающих обработку персональных данных. Сокращение бюджетов в период кризиса еще больше осложнило запуск и выполнение проектов в области защиты персональных данных, а сокращение персонала породило дополнительные риски в области информационной безопасности.

В некоторых организациях бытует представление о том, что усилия регулятора в данной области на проверку окажутся не более чем очередной агитационной кампанией. Однако уже начавшиеся проверки отечественных предприятий Роскомнадзором заставляют сильно усомниться в обоснованности подобной точки зрения. Некоторые руководители полагают, что их предприятие проверки обойдут стороной или что выполнить требования законодательства удастся в последний момент. В действительности же обеспечение защиты персональных данных - от выбора сертифицированных средств защиты либо получения сертификатов ФСБ до развертывания полномасштабной системы защиты, перестройки сопутствующих бизнес-процессов и аудита средств информационной безопасности - требует значительных ресурсов, в том числе и временных.

Контроль за соответствием обработки персональных данных требованиям законодательства осуществляют регуляторы

- **ФСБ России,**
- **Федеральная служба по техническому и экспортному контролю (ФСТЭК),**
- **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).**

Несоблюдение и/или нарушение требований по защите персональных данных может привести к следующим последствиям:

- судебные иски к учреждениям со стороны их сотрудников, партнеров и посетителей;
- принудительное приостановление (до 90 суток) или прекращение обработки персональных данных (что блокирует всю текущую деятельность ЛПУ);
- приостановление действия или аннулирование лицензии на основной вид деятельности учреждения;
- привлечение учреждения и/или его руководителя к гражданской, административной и уголовной ответственности.

Построение системы защиты персональных данных позволяет решить следующие задачи:

- категоризация персональных данных, обрабатываемых в организации
- обоснование классов информационных систем организации, обрабатывающих персональные данные
- определение несоответствий в организации требованиям законодательства и руководящих документов регулирующих органов (ФСБ и ФСТЭК России) в части защиты персональных данных
- формирование требований к построению системы защиты персональных данных
- устранение выявленных в организации несоответствий требованиям законодательства и руководящих документов регулирующих органов (ФСБ и ФСТЭК России)

- подтверждение соответствия процессов обработки персональных данных требованиям №152-ФЗ (декларирование соответствия требованиям по безопасности информации /аттестация ИСПДн по требованиям безопасности информации)

- направление в уполномоченный орган по защите прав субъектов персональных данных официального «Уведомления о начале обработки персональных данных»

Для быстрого и безошибочного решения всех подобных задач и разработан пакет услуг по защите ПДн.

Услуги по защите персональных данных, оказываемые

ЗАО "Проминформ":

- определение требований нормативных правовых актов Российской Федерации для информационной системы в зависимости от состава обрабатываемой информации и принципов обработки;

- проведение классификации информационной системы персональных данных;

- проведение комплексного обследования информационной системы (категорирование информационных ресурсов, определение принципов функционирования информационной системы и технологий обработки информации);

- определение перечня актуальных угроз безопасности информации, анализ угроз безопасности информации, разработка модели угроз безопасности информации;

- выработка рекомендаций по обеспечению безопасности информации;

- разработка организационно-распорядительных документов (инструкций, регламентов), определяющих порядок обработки и обеспечения безопасности персональных данных в организации;

- разработка технического задания на систему защиты персональных данных;

- разработка проекта системы защиты персональных данных;

- поставка, установка и настройка средств защиты информации, ввод в эксплуатацию системы защиты персональных данных;

- техническое обслуживание системы защиты персональных данных;

подготовка необходимой документации и проведение оценки соответствия информационной системы персональных данных требованиям безопасности информации (аттестация информационной системы персональных данных).

ЛИТЕРАТУРА И ИНТЕРНЕТ ИСТОЧНИКИ

Источники:

http://stavkombez.ru/method/PASOIB/html/content/lect_2.html

<http://www.npp-bit.ru/katalog2/po/>

<http://www.paragon.ru>

<http://www.viruslab.ru>

**Лаптев Владимир Николаевич
Лаптев Сергей Владимирович**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Справочник по программно-аппаратным средствам защиты информации
(для бакалавров специальности 080500.62 – Бизнес информатика)

Лицензия ИД № 02334 от 14.07.2000

Подписано в печать
Бумага офсетная
Печ.л. 4,0
Тираж экз.

Формат 60х84
Офсетная печать
Заказ №

Отпечатано в типографии КубГАУ, 350044, г. Краснодар, ул. Калинина, 13