ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Высокий темп внедрения вычислительных средств во все сферы жизнедеятельности человека стал причиной стремительного повышения количества угроз безопасности людей. Это связано с тем, что информация, как результат автоматизированной обработки, с каждым годом определяет действия не только все большего числа людей, но и все большего числа технических систем, созданных человеком. Отсюда становятся понятны последствия потери, подлога или хищения данных, хранящихся в вычислительных системах, а также нарушения работоспособности самих вычислительных средств.

Одним из основных видов угроз целостности и конфиденциальности информации, а также работоспособности вычислительных систем являются преднамеренные угрозы, реализация которых заранее планируется злоумышленником для нанесения вреда. Этот вид угроз по субъекту непосредственной реализации можно разделить на две группы:

- ♦ угрозы, реализация которых выполняется при постоянном участии человека;
- ♦ угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.

Первый тип угроз называют угрозами несанкционированных действий со стороны людей, а второй – со стороны программ, созданных людьми.

Задачи по защите от реализации угроз каждого из данных типов одинаковы:

1. преградить несанкционированный доступ к ресурсам вычислительных систем;
2. сделать невозможным несанкционированное использование компьютерных ресурсов, если доступ к ним все-таки осуществлен;
3. своевременно обнаружить факт несанкционированных действий устранить причины, а также последствия их реализации.

Способы же решения перечисленных задач по защите от несанкционированных действий со стороны людей и компьютерных программ существенно отличаются друг от друга.

Данное пособие посвящено рассмотрению основных способов защиты от несанкционированных действий, реализуемых при непосредственном участии человека.

Основными функциями системы защиты по преграждению несанкционированного доступа людей к ресурсам вычислительных систем являются, прежде всего, идентификация и подтверждение подлинности пользователей при доступе в вычислительную систему, а также разграничение их доступа к компьютерным ресурсам. Важную роль играет также функция корректного завершения сеанса работы пользователей,

предотвращающая возможность реализации угрозы маскировки под санкционированного пользователя вычислительной системы. Обычное завершение сеанса работы должно обязательно проводиться каждым пользователем по окончании его работы. Принудительное же завершение сеанса работы или блокировка устройств ввода-вывода должны выполняться по истечении для пользователя заданного времени бездействия (отсутствия признаков активности).

1 Основные этапы допуска в компьютерную систему

Системой защиты по отношению к любому пользователю с целью обеспечения безопасности обработки и хранения информации должны быть предусмотрены следующие этапы допуска в вычислительную систему:

1. идентификация;
2. установление подлинности (аутентификация);
3. определение полномочий для последующего контроля и разграничения доступа к компьютерным ресурсам (авторизация).

Данные этапы должны выполняться и при подключении к компьютерной системе (КС) таких устройств, как удаленные рабочие станции и терминалы.

Идентификация необходима для указания компьютерной системе уникального идентификатора обращающегося к ней пользователя с целью выполнения следующих защитных функций:

- ♦ установление подлинности и определение полномочий пользователя при его допуске в компьютерную систему;
- ♦ контроль установленных полномочий и регистрация заданных действий пользователя в процессе его сеанса работы после допуска данного пользователя в КС;
- ♦ учет обращений к компьютерной системе.

Сам идентификатор может представлять собой последовательность любых символов и должен быть заранее зарегистрирован в системе администратором службы безопасности. В процессе регистрации администратором в базу эталонных данных системы защиты для каждого пользователя заносятся следующие элементы данных:

- ♦ фамилия, имя, отчество и, при необходимости, другие характеристики пользователя;
- ♦ уникальный идентификатор пользователя;
- ♦ имя процедуры установления подлинности;
- ♦ используемая для подтверждения подлинности эталонная информация, например, пароль;
- ♦ ограничения на используемую эталонную информацию, например, минимальное и максимальное время, в течение которого указанный пароль будет считаться действительным;
- ♦ полномочия пользователя по доступу к компьютерным ресурсам.

Процесс установления подлинности, называемый еще аутентификацией, заключается в проверке, является ли пользователь, пытающийся осуществить доступ в КС, тем, за кого себя выдает.

Общая схема идентификации и установления подлинности пользователя при его доступе в компьютерную систему представлена на рисунке 1.

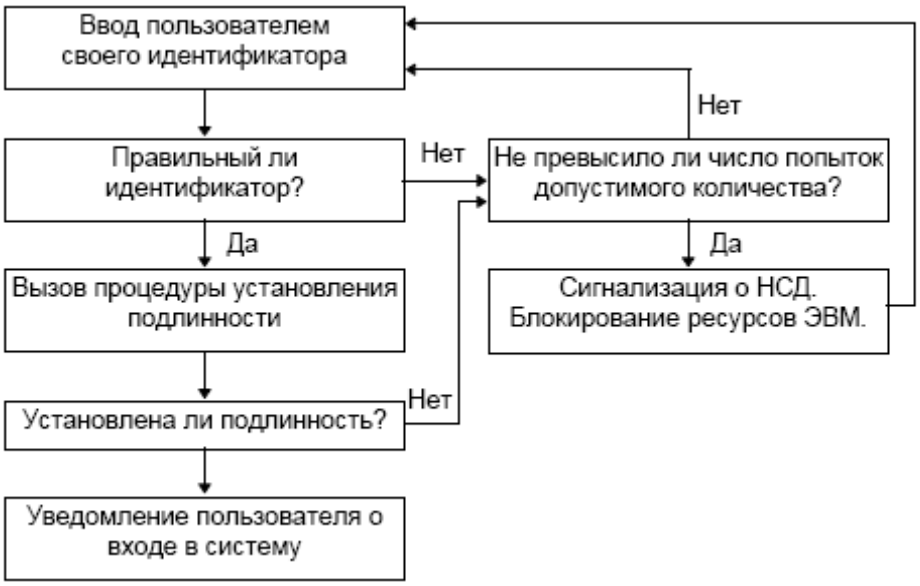


Рисунок 1. Схема идентификации и аутентификации пользователя при его доступе в КС

Если в процессе аутентификации подлинность пользователя установлена, то система защиты должна определить его полномочия по использованию ресурсов КС для последующего контроля установленных полномочий.

Основными и наиболее часто применяемыми методами установления подлинности пользователей являются методы, основанные на использовании паролей. Под паролем при этом понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к компьютерной системе. Ввод пароля, как правило, выполняют с клавиатуры после соответствующего запроса системы.

Эффективность парольных методов может быть значительно повышена путем записи в зашифрованном виде длинных и нетривиальных паролей на информационные носители, например, дискеты, магнитные карты, носители данных в микросхемах и т.д. В этом случае компьютерная система должна включать специальные устройства и обслуживающие их драйверы для считывания паролей с этих информационных носителей, а служба безопасности должна располагать средствами для формирования носителей с парольными данными.

Для особо надежного опознавания могут применяться и методы, основанные на использовании технических средств определения сугубо индивидуальных характеристик человека (голоса, отпечатков пальцев, структуры зрачка и т.д.). Однако такие средства требуют значительных затрат и поэтому используются редко.

Существующие парольные методы проверки подлинности пользователей при входе в КС можно разделить на две группы:

♦ методы проверки подлинности на основе простого пароля;

- ♦ методы проверки подлинности на основе динамически изменяющегося пароля.

Пароль подтверждения подлинности пользователя при использовании простого пароля не изменяется от сеанса к сеансу в течении установленного администратором службы безопасности времени его существования (действительности).

При использовании динамически изменяющегося пароля пароль пользователя для каждого нового сеанса работы или нового периода действия одного пароля изменяется по правилам, зависящим от используемого метода.

2 Использование простого пароля

Процедура опознавания с использованием простого пароля может быть представлена в виде следующей последовательности действий:

1. пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;
2. система запрашивает пароль;
3. пользователь вводит пароль;
4. система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

Поскольку пользователь может допустить ошибку при вводе пароля, то системой должно быть предусмотрено допустимое количество повторений для ввода пароля.

В базе эталонных данных системы защиты пароли, как и другую информацию, никогда не следует хранить в явной форме, а только зашифрованными. При этом можно использовать метод как обратимого, так и необратимого шифрования.

Согласно методу обратимого шифрования эталонный пароль при занесении в базу эталонных данных зашифровывается по ключу, совпадающему с этим эталонным паролем, а введенный после идентификации пароль пользователя для сравнения с эталонным также зашифровывается, но по ключу, совпадающему с этим введенным паролем. Таким образом, при сравнении эталонный и введенный пароли находятся в зашифрованном виде и будут совпадать только в том случае, если исходный введенный пароль совпадет с исходным эталонным. При несовпадении исходного введенного пароля с исходным эталонным исходный введенный пароль будет зашифрован по другому, так как ключ шифрования отличается от ключа, которым зашифрован эталонный пароль, и после зашифровывания не совпадет с зашифрованным эталонным паролем.

Для обеспечения возможности контроля правильности ввода пароля при использовании необратимого шифрования на винчестер записывается таблица преобразованных паролей. Для их преобразования используется односторонняя криптографическая функция $y=F(x)$, обладающая следующим свойством: для данного аргумента x значение $F(x)$ вычисляется легко, а по данному y вычислительно сложно найти значение аргумента x, соответствующего данному y. В таблице паролей хранятся значения односторонних функций, для которых пароли берутся в качестве аргументов. При вводе пароля система защиты легко вычисляет значение функции от пароля текущего пользователя и сравнивает со значением, приведенным в таблице для пользователя с выбранным идентификатором. Нарушитель,

захвативший компьютер, может прочитать таблицу значений функций паролей, однако вычисление пароля практически не реализуемо.

При работе с паролями должна предусматриваться и такая мера, как недопустимость их распечатки или вывода на экраны мониторов. Поэтому система защиты должна обеспечивать ввод пользователями запрошенных у них паролей без отображения этих паролей на мониторах.

Можно выделить следующие основные способы повышения стойкости системы защиты на этапе аутентификации:

- ♦ повышение степени нетривиальности пароля;
- ♦ увеличение длины последовательности символов пароля;
- ♦ увеличение времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля;
- ♦ повышение ограничений на минимальное и максимальное время действительности пароля.

Чем нетривиальнее пароль, тем сложнее его запомнить. Плохо запоминаемый пароль может быть записан на листе бумаги, что повышает риск его раскрытия. Выходом здесь является использование определенного числа не записываемых на бумаге пробелов или других символов в начале, внутри, а также в конце последовательности основных символов пароля. Кроме того, отдельные символы пароля могут набираться на другом регистре (например, вместо строчных набираться прописными или наоборот), что также не должно отражаться на листе бумаги. В этом случае незаконно полученный лист бумаги с основными символами пароля не будет достаточным условием раскрытия пароля целиком.

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля. Ожидаемое время раскрытия пароля T_r можно вычислить на основе следующей полученной экспериментально приближенной формулы:

$T_r \approx (A_s * T_v)/2$.

Здесь:

A - число символов в алфавите, используемом для набора символов пароля;

S - длина пароля в символах, включая пробелы и другие служебные символы;

T_v - время ввода пароля с учетом времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля.

Например, если A = 26 символов (учтены только буквы английского алфавита), T_v = 2 секунды, а S = 6 символов, то ожидаемое время раскрытия T_r приблизительно равно одному году. Если в данном примере после каждой неудачной попытки ввода пароля предусмотреть временную задержку в 10 секунд, то ожидаемое время раскрытия увеличится в 5 раз.

Из приведенной выше формулы становится понятно, что повышения стойкости системы защиты на этапе аутентификации можно достигнуть и увеличением числа символов алфавита, используемого для набора символов пароля. Такое увеличение можно обеспечить путем использования нескольких регистров (режимов ввода) клавиатуры для набора символов пароля, например, путем использования строчных и прописных латинских символов, а также строчных и прописных символов кириллицы.

Для исключения необходимости запоминания пользователями длинных и нетривиальных паролей в системе защиты может быть предусмотрена возможность записи паролей в зашифрованном виде на информационные носители, например, дискеты, магнитные карты, носители данных в микросхемах и т.д., а также считывания паролей с этих информационных носителей. Такая возможность позволяет повысить безопасность за счет значительного увеличения длины паролей, записываемых на носители информации. Однако при этом администрации службы безопасности следует приложить максимум усилий для разъяснения пользователям КС о необходимости тщательной сохранности носителей информации с их паролями.

На степень информационной безопасности при использовании простого парольного метода проверки подлинности пользователей большое влияние оказывают ограничения на минимальное и максимальное время действительности каждого пароля. Чем чаще меняется пароль, тем большая безопасность обеспечивается.

Минимальное время действительности пароля задает время, в течение которого пароль менять нельзя, а максимальное - время, по истечении которого пароль будет недействительным. Соответственно, пароль должен быть заменен в промежутке между минимальным и максимальным временем его существования. Поэтому понятно, что более частая смена пароля обеспечивается при уменьшении минимального и максимального времени его действительности.

Минимальное и максимальное время действительности пароля задаются для каждого пользователя администратором службы безопасности, который должен постоянно контролировать своевременность смены паролей пользователей.

3 Использование динамически изменяющегося пароля

Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, так как частота смены паролей в них максимальна – пароль для каждого пользователя меняется ежедневно или через несколько дней. При этом каждый следующий пароль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

Существуют следующие методы парольной защиты, основанные на использовании динамически изменяющегося пароля:

- ♦ методы модификации схемы простых паролей;
- ♦ метод «запрос-ответ»;
- ♦ функциональные методы.

Наиболее эффективными из данных методов, как станет понятно далее, являются функциональные методы.

3.1 Методы модификации схемы простых паролей

К методам модификации схемы простых паролей относят случайную выборку символов пароля и одноразовое использование паролей.

При использовании первого метода каждому пользователю выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только его некоторая часть. В процессе проверки подлинности система запрашивает у пользователя группу символов по заданным порядковым номерам. Количество символов и их порядковые номера для запроса определяются с помощью датчика псевдослучайных чисел.

При одноразовом использовании паролей каждому пользователю выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки.

Недостатком методов модификации схемы простых паролей является необходимость запоминания пользователями длинных паролей или их списков. Запись же паролей на бумагу или в записные книжки приводит к появлению риска потери или хищения носителей информации с записанными на них паролями.

3.2 Метод «запрос-ответ»

При использовании метода «запрос-ответ» в КС заблаговременно создается и особо защищается массив вопросов, включающий в себя как

вопросы общего характера, так и персональные вопросы, относящиеся к конкретному пользователю, например, вопросы, касающиеся известных только пользователю случаев из его жизни.

Для подтверждения подлинности пользователя система последовательно задает ему ряд случайно выбранных вопросов, на которые он должен дать ответ. Опознание считается положительным, если пользователь правильно ответил на все вопросы.

Основным требованием к вопросам в данном методе аутентификации является уникальность, подразумевающая, что правильные ответы на вопросы знают только пользователи, для которых эти вопросы предназначены.

3.3 Функциональные методы

Среди функциональных методов наиболее распространенными являются метод функционального преобразования пароля, а также метод «рукопожатия».

Метод функционального преобразования основан на использовании некоторой функции F, которая должна удовлетворять следующим требованиям:

- для заданного числа или слова X легко вычислить Y=F(X);
- зная X и Y сложно или невозможно определить функцию Y=F(X).

Необходимым условием выполнения данных требований является наличие в функции F(X) динамически изменяющихся параметров, например, текущих даты, времени, номера дня недели, или возраста пользователя.

Пользователю сообщается:

- исходный пароль - слово или число X, например число 31;
- функция F(X), например, Y=(X mod 100) * D + W3, где (X mod 100) - операция взятия остатка от целочисленного деления X на 100, D - текущий номер дня недели, а W - текущий номер недели в текущем месяце;
- периодичность смены пароля, например, каждый день, каждые три дня или каждую неделю.

Паролями пользователя для последовательности установленных периодов действия одного пароля будут соответственно X, F(X), F(F(X)), F(F(F(X))) и т.д., т.е. для i-го периода действия одного пароля паролем пользователя будет $F^{i-1}(X)$. Поэтому для того, чтобы вычислить очередной пароль по истечении периода действия используемого пароля пользователю не нужно помнить начальный (исходный) пароль, важно лишь не забыть функцию парольного преобразования и пароль, используемый до настоящего момента времени.

С целью достижения высокого уровня безопасности функция преобразования пароля, задаваемая для каждого пользователя, должна периодически меняться, например, каждый месяц. При замене функции целесообразно устанавливать и новый исходный пароль.

Согласно методу «рукопожатия» существует функция F, известная только пользователю и КС. Данная функция должна удовлетворять тем же требованиям, которые определены для функции, используемой в методе функционального преобразования.

При входе пользователя в КС системой защиты генерируется случайное число или случайная последовательность символов X и вычисляется функция F(X), заданная для данного пользователя (см. рис. 2). Далее X выводится пользователю, который должен вычислить F'(X) и ввести полученное значение в систему. Значения F(X) и F'(X) сравниваются системой и если они совпадают, то пользователь получает доступ в КС.

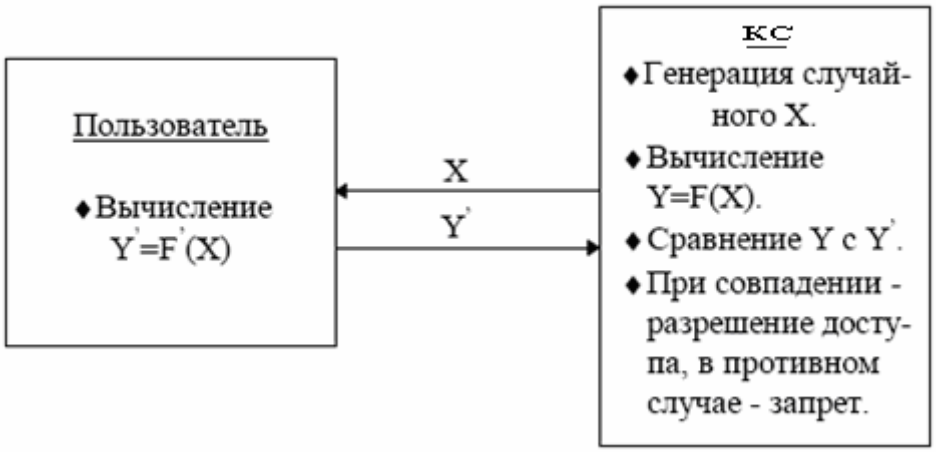


Рисунок 2. Схема аутентификации по методу «рукопожатия»

Например, в КС генерируется и выдается пользователю случайное число, состоящее из семи цифр. Для заблуждения злоумышленника в любое место числа может вставляться десятичная точка. В качестве функции F принимается: Y = (<сумма 1-й, 2-й и 5-й цифр числа>)^2 - <сумма 3-й, 4-й, 6-й и 7-й цифр числа> + <сумма цифр текущего времени в часах>.

Для высокой безопасности функцию «рукопожатия» целесообразно циклически менять через определенные интервалы времени, например, устанавливать разные функции для четных и нечетных чисел месяца.

Достоинством метода «рукопожатия» является то, что никакой конфиденциальной информации между пользователем и КС не передается. По этой причине эффективность данного метода особенно велика при его применении в вычислительных сетях для подтверждения подлинности пользователей, пытающихся осуществить доступ к серверам или центральным ЭВМ.

В некоторых случаях может оказаться необходимым пользователю проверить подлинность той КС, к которой он хочет осуществить доступ. Необходимость во взаимной проверке может понадобиться и когда два пользователя КС хотят связаться друг с другом по линии связи. Методы простых паролей, а также методы модификации схем простых паролей в этом случае не подходят. Наиболее подходящим здесь является метод «рукопожатия». При его использовании ни один из участников сеанса связи не будет получать никакой конфиденциальной информации.

4 Предотвращение несанкционированного доступа к персональному компьютеру

4.1 Защита от несанкционированного входа в компьютерную систему

Для защиты от несанкционированного входа в персональную компьютерную систему могут использоваться как общесистемные, так и специализированные программные средства защиты.

К общесистемным средствам относится утилита Setup, входящая в состав BIOS и предназначенная для настроек аппаратных параметров компьютера. Для реализации рассматриваемого вида защиты необходимо с помощью данной утилиты установить следующие параметры загрузки компьютера:

- ♦ порядок загрузки операционной системы (ОС), задающий первичную загрузку с жесткого диска (устройства C:);
- ♦ запрос пароля перед загрузкой операционной системы.

Установка первичной загрузки с жесткого диска необходима для предотвращения возможности загрузки ОС с дискеты или компакт-диска, так как некоторые устаревшие версии BIOS позволяют осуществить загрузку с дискеты без запроса пароля. Если используемая версия BIOS при установленном пароле загрузки обеспечивает запрос пароля и при загрузке с дискеты, что, как правило, реализовано во всех современных версиях базовой системы ввода-вывода, то изменять порядок загрузки для защиты от несанкционированного входа в компьютерную систему нет необходимости.

Запуск утилиты Setup выполняется, как правило, нажатиями клавиши Del после активизации процесса загрузки операционной системы, т.е. после включения компьютера или нажатия кнопки Reset в процессе сеанса работы пользователя.

После запуска утилиты необходимо войти в пункт меню «BIOS Features Setup» («Advanced CMOS Setup») и с помощью клавиш PgUp и PgDn установить следующие переключатели:

- ♦ «Boot Sequence» («System Boot Up Sequence») - в положение «C, A» или «C, CDROM, A»;
- ♦ «Security Option» («Password Checking Options») - в положение «System».

Далее следует задать пароль входа в систему с помощью пункта меню «Password Setting» («Change Password»), а потом сохранить сделанные изменения и выйти из утилиты с помощью пункта меню «Save & Exit Setup».

Выполнив указанные действия, загрузка компьютера будет выполняться только после ввода правильного пароля.

При необходимости изменения пароля следует активизировать утилиту Setup, изменить пароль с помощью пункта меню «Password Setting» («Change Password»), а потом сохранить сделанные изменения и выйти из утилиты с помощью пункта меню «Save & Exit Setup».

Недостатком реализации защиты от несанкционированной загрузки компьютера с помощью утилиты BIOS Setup является то, что установленная с помощью данной утилиты защита может быть преодолена путем принудительного обнуления содержимого энергонезависимой памяти компьютера (CMOS-памяти) после вскрытия его корпуса.

Для эффективной защиты необходимо использование наложенных средств защиты информации, например, программно-аппаратного комплекса «Соболь» («Соболь 3.0», «Соболь 2.1», «Соболь 2.0»), который позволяет реализовать один из следующих режимов входа пользователя:

- **Стандартный** – Для входа в систему пользователь должен ввести свои учетные данные, используя только стандартные средства ОС Windows;
- **Смешанный** – Для входа в систему пользователь может предъявить персональный аппаратный идентификатор (iButton, eToken PRO, iKey 2032, Rutoken S или Rutoken RF S), активированный средствами «Соболь», или ввести свои учетные данные, используя стандартные средства ОС Windows;
- **Только по идентификатору** – Для входа в систему пользователь должен предъявить персональный аппаратный идентификатор, активированный средствами «Соболь». Пользователи, не имеющие персонального идентификатора, войти в систему не смогут. Администратор может войти в систему без предъявления идентификатора только в административном режиме вход в систему при условии раздельного ввода независимыми субъектами двух разных паролей.

Кроме того, программно-аппаратный комплекс «Соболь» позволяет реализовать один из двух режимов аутентификации пользователя:

- **Стандартная аутентификация** – Выполняется по паролю пользователя;
- **Усиленная аутентификация по ключу** – Кроме пароля проверяется подлинность и актуальность (т. е. срок действия) закрытого ключа пользователя. Для загрузки закрытого ключа пользователь должен предъявить персональный идентификатор. Если подтверждаются подлинность и актуальность ключа, пользователю разрешается вход в систему. Если подлинность ключа не подтверждается, вход запрещается и регистрируется значение ключа. Если срок действия ключа истек, пользователю предлагается выполнить смену ключей для усиленной аутентификации.

4.2 Защита от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы

В ряде случаев в процессе работы пользователя за компьютером может возникнуть необходимость кратковременно оставить компьютер без присмотра, не завершая при этом сеанс работы (не выключая компьютер). При отсутствии пользователя ничто не мешает осуществлению несанкционированного доступа к компьютерной системе, так как процесс подтверждения подлинности уже выполнен санкционированным пользователем, оставившим компьютер.

Для предотвращения такой ситуации перед оставлением компьютера необходимо либо завершить сеанс работы, либо заблокировать клавиатуру, мышь и экран до активизации процесса подтверждения подлинности. Кроме того, должна быть предусмотрена возможность автоматического блокирования клавиатуры, мыши и экрана по истечении заданного времени бездействия пользователя. Это обеспечит защиту, если при оставлении компьютера пользователь забудет завершить сеанс работы или принудительно заблокировать клавиатуру, мышь и экран.

В ОС Windows возможна реализация защиты от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы. Для этого в ОС Windows XP необходимо выполнить следующие действия:

1. активизация «Панели управления» Windows XP и запуск программного компонента «Экран», предназначенного для настройки параметров экрана;
2. активизация листа свойств «Заставка» (см. рис. 3) и выбор понравившегося хранителя экрана;
3. установка в поле «Интервал» требуемого времени бездействия пользователя, по истечении которого будет активизироваться хранитель экрана;
4. установка флажка «Защита паролем»;
5. подтверждение нажатием кнопки ОК внесенных изменений и закрытие «Панели управления».

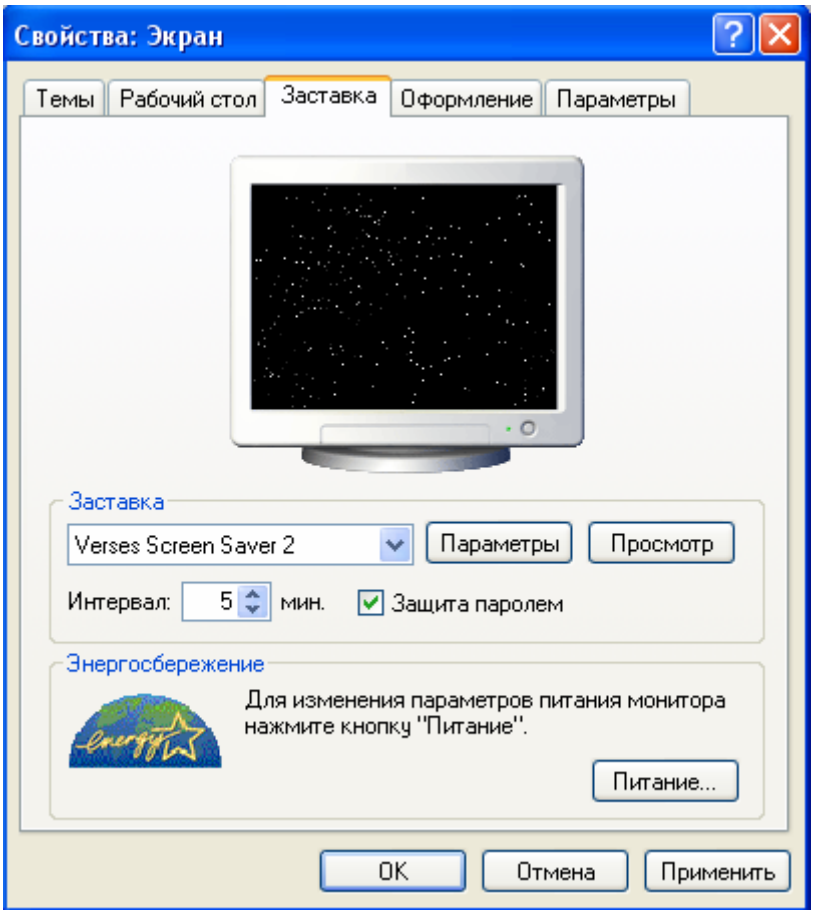


Рисунок 3. Лист свойств «Заставка»

После выполнения указанных настроек по истечении установленного времени бездействия пользователя будет активизирован хранитель экрана, который не позволит вернуться в систему без ввода заданного в «Панели управления» пароля. Изменение пароля возврата в систему осуществляется по аналогии с процессом его установки.

5 Способы разграничения доступа

После идентификации и аутентификации пользователя система защиты должна определить его полномочия для последующего контроля санкционированности доступа к компьютерным ресурсам. Полномочия пользователя считываются из базы эталонных данных системы защиты и заносятся в базу данных активных пользователей, которая для достижения более высокой производительности компьютера может располагаться в разделах его оперативной памяти.

При функционировании компьютера система защиты должна постоянно контролировать правомерность доступа пользователей к ресурсам вычислительной системы. Для этого при попытке доступа любого пользователя к какому-либо компьютерному ресурсу система защиты должна проанализировать полномочия этого пользователя, считав их из базы данных активных пользователей, и разрешить доступ только в случае соответствия запроса на доступ пользовательским полномочиям. В случае многопользовательского режима работы компьютера (сервера) для определения системой защиты идентификатора пользователя, пытающегося осуществить доступ к ресурсу, каждой запущенной программе присваивается идентификатор пользователя, который ее запустил.

Процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам называют разграничением доступа, а подсистему защиты, выполняющую эти функции - подсистемой разграничения доступа пользователей к ресурсам КС. Эффективной может быть только та политика разграничения доступа, в основу которой положен принцип - «запрещено все, что не разрешено», а не «разрешено все, что не запрещено».

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

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

Информация о полномочиях пользователей по использованию ресурсов КС вносится в базу эталонных данных системы защиты администратором службы безопасности при регистрации этого пользователя после задания для

него уникального идентификатора. Полномочия пользователя включают следующие элементы данных:

- ♦ список ресурсов, к которым доступ пользователю разрешен;
- ♦ права по доступу к каждому ресурсу из списка.

В качестве ресурсов КС, полномочия, на которые определяются в базе эталонных данных системы защиты, могут выступать любые компьютерные ресурсы, а именно:

- ♦ программы;
- ♦ внешняя память (файлы, каталоги, логические диски и др.);
- ♦ информация, разграниченная по категориям в базах данных;
- ♦ оперативная память;
- ♦ время процессора или приоритет по использованию его времени;
- ♦ порты ввода-вывода;
- ♦ внешние устройства, например, принтеры.

Различают следующие виды прав пользователей по доступу к конкретному ресурсу:

- ♦ всеобщее право, когда ресурс полностью предоставляется в распоряжение пользователя (например, полное предоставление накопителя для гибких дискет);
- ♦ функциональное или частичное право, когда в распоряжение пользователя предоставляются только отдельные функции или части запрашиваемого ресурса (например, предоставление одного из логических дисков винчестера);
- ♦ временное право, когда ресурс предоставляется на некоторое время либо его функции или размер зависят от времени, например, времени суток, дня недели или месяца.

Кроме того, отдельным пользователям КС могут предоставляться полномочия по управлению и установлению полномочий других пользователей.

В базе эталонных данных системы защиты могут быть определены также ограничения на пользовательские полномочия, например, зависимость полномочий от территориального расположения или вида узла сети в распределенной вычислительной системе.

Существуют различные способы разграничения доступа к ресурсам КС, каждый из которых определяет структуру информации о пользовательских полномочиях в базе эталонных данных системы защиты, а также способы использования данной информации при определении полномочий каждого пользователя и их контроле.

Наиболее распространенными являются следующие способы:

- ♦ разграничение доступа по спискам;
- ♦ использование матрицы установления полномочий;
- ♦ разграничение доступа по уровням секретности и категориям;

♦ парольное разграничение доступа.

Каждый из перечисленных методов обладает своими достоинствами и недостатками. Наибольший же эффект достигается при их комплексном использовании.

5.1 Разграничение доступа по спискам

При разграничении доступа по спискам для каждого пользователя задается список ресурсов и прав доступа к ним или для каждого ресурса задается список пользователей их прав доступа к данному ресурсу. Например, для пользователя, идентификатор которого User_1, в базе эталонных данных задается список, определяющий, что он имеет доступ к каталогу User_1 логического диска привода D:, а также к текстовому редактору Office Word 2007.

Процедура разграничения при использовании списков выполняется в следующей последовательности.

1. По данным, содержащимся в запросе пользователя, выбирается соответствующая строка списка:
   - либо список ресурсов, к которым данный пользователь имеет доступ и прав доступа к ним;
   - либо список пользователей, которым разрешен доступ к запрашиваемому ресурсу и прав их доступа.
2. В выбранной строке проверяется наличие запрашиваемого ресурса или идентификатора пользователя, выдавшего запрос.
3. Если наличие установлено и тип запрашиваемого доступа соответствует правам пользователя, то ресурс предоставляется в соответствии с правами доступа на него. В противном случае доступ пользователя к запрашиваемому ресурсу блокируется и применяются санкции, предусмотренные за попытку несанкционированного доступа.

5.2 Использование матрицы установления полномочий

Разграничение доступа на основе матрицы установления полномочий является более гибким и удобным в сравнении с разграничением по спискам, так как позволяет всю информацию о пользовательских полномочиях в базе эталонных данных системы защиты хранить и использовать в виде матриц (таблиц), а не в виде разнотипных списков.

В матрице, или как ее еще называют, таблице полномочий строками являются идентификаторы пользователей, имеющих доступ в систему, а столбцами - ресурсы вычислительной системы. Каждая ячейка таблицы для

заданного пользователя и ресурса может содержать следующую информацию:

- ♦ размер предоставляемого ресурса, например, размер области внешней памяти;
- ♦ имя компонента предоставляемого ресурса, например, имя каталога или логического диска;
- ♦ код, определяющий права доступа к ресурсу, например, 01_2 -только чтение, 10_2 - чтение и запись и т.д.;
- ♦ ссылку на другую информационную структуру, задающую права доступа к ресурсу, например, ссылку на другую матрицу полномочий;
- ♦ ссылку на программу, регулирующую права доступа к ресурсу.

Программа, регулирующая права доступа пользователя к ресурсу, может регулировать права доступа не только в зависимости от времени, но и в зависимости от предыстории работы пользователя, например, пользователь User_33 может записывать данные в файл F только в том случае, если он уничтожил файл G. Также может учитываться и состояние КС, например, текущий размер свободной части ресурса.

В качестве простейшего примера матрицы полномочий можно привести следующую таблицу:

	Каталог D:\WORK	Каталог D:\BOOK	Каталог D:\TEST
Пользователь User_1	10	01	10
Пользователь User_2	10	10	00
Пользователь User_3	00	10	01
……..		……	
Пользователь User_N	10	00	00

В данной таблице каждая ячейка содержит двоичный код, задающий права доступа к ресурсу: 01 - только чтение, 10 - чтение и запись, а 00 - запрет доступа.

Упрощенная схема обработки запроса на доступ к ресурсу при использовании матрицы установления полномочий представлена на рисунке 4.

Недостатком метода разграничения доступа на основе матрицы полномочий является то, что для большой КС данная матрица может оказаться слишком громоздкой. Преодолеть данный недостаток можно путем выполнения следующих рекомендаций по сжатию матрицы установления полномочий:

- ♦ объединение пользователей, имеющих идентичные полномочия в группы;
- ♦ объединение ресурсов, полномочия на доступ к которым совпадают;

♦ комбинирование метода разграничения доступа на основе матрицы полномочий с методом разграничения по уровням секретности.

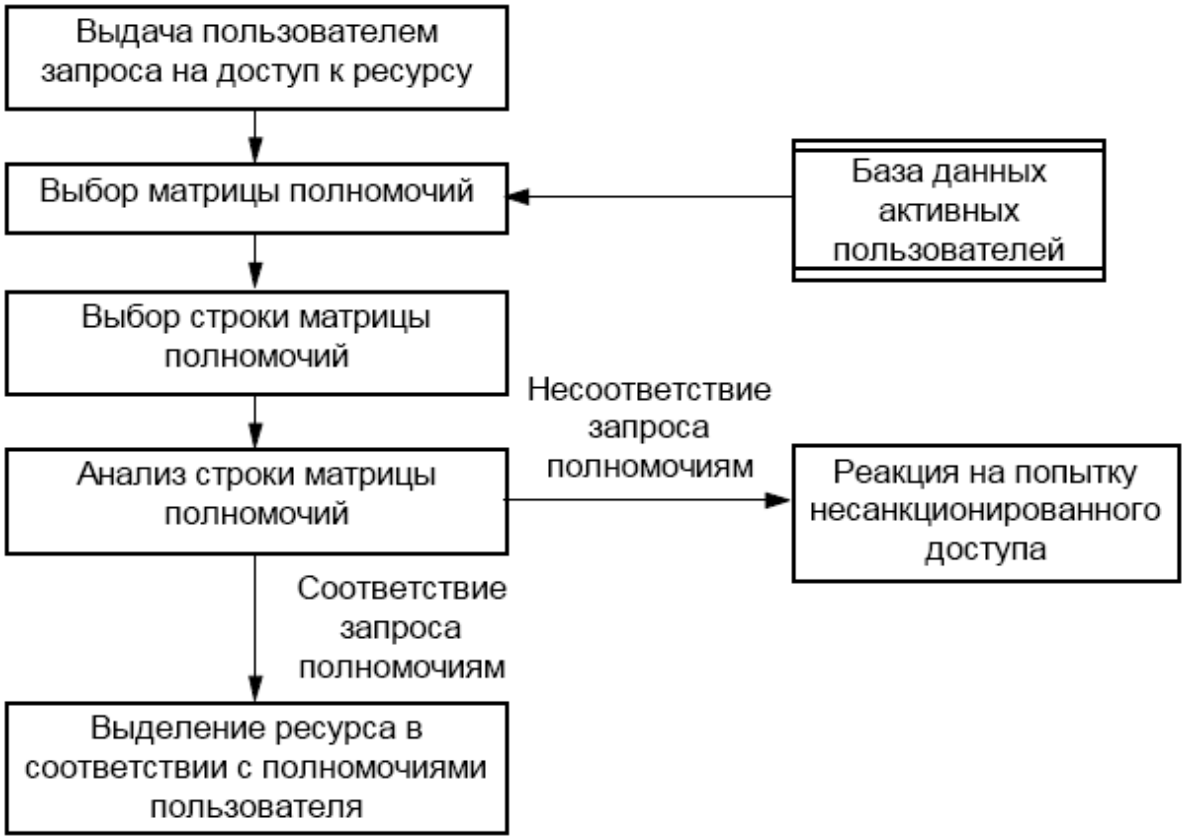


Рисунок 4. Схема обработки запроса на доступ к ресурсу при использовании матрицы полномочий

В ОС Linux права доступа к файлу или к каталогу описываются тремя (вообще-то больше, хотя эти три основные и самые важные) восьмеричными цифрами, самая левая из этой тройки – права владельца, средняя – права группы, правая – права всех остальных. Каждая из этих восьмеричных цифр представляет собой битовую маску из трех битов. Эти биты отвечают за права на (слева направо) чтение, запись и исполнение файла или каталога. Если установлена единица – доступ разрешен, если ноль – запрещен. Таким образом, права доступа к файлу, описанные цифрой 644, означают, что владелец может писать и читать файл, группа и остальные пользователи – только читать. С точки зрения функциональных возможностей

1. чтение означает:

♦ просмотр содержимого файла,

♦ чтение каталога,

2. запись означает:

♦ добавление или изменение файла,

♦ удаление или перемещение файлов в каталоге,

3. выполнение файла означает:

♦ запуск программы,

♦ возможность поиска в каталоге в комбинации с правом чтения.

Узнать о том, какие права доступа установлены к файлам и каталогам, можно, используя команду *ls*.

5.3 Разграничение доступа по уровням секретности и категориям

Разграничение доступа по уровням секретности заключается в том, что такие ресурсы вычислительной системы, как логические диски, каталоги, файлы, а также элементы баз данных разделяются на группы в соответствии с уровнями их секретности. В качестве таких уровней могут быть выделены следующие:

♦ «общий доступ»;

♦ «конфиденциально»;

♦ «секретно»;

♦ «совершенно секретно».

Полномочия каждого пользователя задаются максимальным уровнем секретности информации, доступ к которой ему разрешен. В соответствии с этим, пользователю разрешается доступ только к данным, уровень секретности которых не выше уровня его полномочий.

Разграничение доступа по категориям состоит в том, что все информационные ресурсы вычислительной системы (логические диски, каталоги, файлы, а также элементы баз данных) разделяются на группы в соответствии с категориями содержащихся в них данных. Например, все тактико-технические данные о средствах вооружения могут быть разделены по типам этих средств - данные о наземных, морских, а также воздушных средствах вооружения.

Полномочия каждого пользователя задаются категориями информации, доступ к которой ему разрешен. В соответствии с этим, пользователю разрешается доступ только к данным, категории которых совпадают с категориями, заданными в его полномочиях.

Важной особенностью разграничения доступа по уровням секретности и категориям, называемым еще мандатным способом разграничения, является то, что всем программам КС должно быть запрещено выполнение следующих действий:

♦ переписывание информации из областей памяти с более высоким уровнем секретности в области памяти с более низким;

♦ переписывание данных из областей памяти, соответствующих одной категории, в области памяти, соответствующие другой.

Здесь в качестве области памяти может выступать как область внешней, так и оперативной памяти. Под областью внешней памяти понимается логический диск, каталог, файл или элемент базы данных, которому присвоен один уровень секретности или одна категория. Под

областью же оперативной памяти - загруженный в оперативную память файл или элемент базы данных, соответствующий одному уровню секретности или одной категории.

Достигнуть требуемой гибкости и детализации при разграничении доступа пользователей к информационным ресурсам крупной КС можно только при совместном использовании способов разграничения доступа по уровням секретности и категориям.

5.4 Парольное разграничение и комбинированные методы

Парольная система разграничения заключается в том, что доступ пользователей к ресурсам разрешается только при условии подтверждения ими санкционированности доступа парольным способом.

В парольном разграничении могут применяться любые методы парольной защиты, которые используются для подтверждения подлинности пользователей при доступе в компьютерную систему. Например, в случае использования простого пароля защищаемому ресурсу ставится в соответствие пароль и доступ пользователя к этому ресурсу разрешается только при условии ввода на запрос совпадающего пароля.

Пароли для доступа к ресурсам выдаются администраторами службы безопасности или владельцами ресурсов. Сама же процедура разграничения является достаточно простой:

1. при попытке доступа пользователя к ресурсу выдается запрос на ввод пароля;
2. предъявленный пользователем пароль сравнивается с текущим эталонным паролем;
3. если пароли совпадают, то доступ к ресурсу разрешается; в противном случае доступ блокируется, и принимаются санкции за попытку несанкционированного доступа.

В связи с тем, что способы доступа к ресурсам КС, для которых установлена парольная защита, полностью аналогичны парольным способам проверки подлинности пользователей при их допуске в компьютерную систему, то здесь могут возникать те же трудности, что и при аутентификации пользователей: утеря, перехват, разгадывание и подбор пароля.

Недостатком парольного разграничения доступа является необходимость временных задержек в работе пользователей для ввода пароля при доступе к ресурсам, защищенным парольным способом. Это в какой-то степени снижает удобство работы пользователей. Поэтому парольное разграничение как самостоятельный способ разграничения доступа на практике используют исключительно редко, а применяют его в основном для защиты особо важных ресурсов КС совместно с другими способами разграничения доступа.

Среди комбинированных способов разграничения наиболее эффективными являются следующие:

- комбинирование разграничения по спискам и парольного разграничения;
- комбинирование матричного и парольного разграничения;
- комбинирование разграничения по уровням секретности и категориям, а также парольного разграничения;

- комбинирование всех рассмотренных методов разграничения доступа - по спискам, матричного, по уровням секретности и категориям, а также парольного разграничения.

Следует учитывать, что в перечисленных комбинированных методах парольное разграничение целесообразно использовать только для тех ресурсов КС, которые требуют максимальной степени защищенности. При этом будет обеспечена двухуровневая защита при несанкционированном доступе пользователя к ресурсу, защищенному одним из перечисленных комбинированных способов:

- на первом уровне система защиты блокирует несанкционированный доступ на основе анализа полномочий пользователей в соответствии с разграничением по спискам, матричным разграничением или разграничением по уровням секретности и категориям;
- на втором уровне для доступа к ресурсу пользователю необходимо подтвердить санкционированность доступа путем ввода запрашиваемого у него пароля. Только при комплексном использовании методов разграничения можно достигнуть высокой степени безопасности защищаемых ресурсов КС и требуемой гибкости при детализации пользовательских полномочий.

6 Программная реализация контроля установленных полномочий

Подсистема разграничения доступа на основе того или иного метода должна осуществлять постоянный контроль установленных полномочий при каждом запросе пользователем ресурса КС.

Этот контроль выполняется на основе реализации двух базовых этапов:

1. анализ полномочий пользователя, который запросил ресурс;
2. предоставление ресурса или запрет доступа в соответствии с результатами анализа.

Возникает вопрос, каким образом передать управление подсистеме разграничения сразу же после выдачи пользователем запроса на доступ к ресурсу КС.

Доступ к ресурсам КС со стороны пользователей может выполняться только через компьютерные программы. Доступ к ресурсам из программ реализуется на основе использования функций операционной системы (ОС). Выполнение же самих функций ОС по доступу к ресурсам КС основано на использовании прерываний в работе центрального процессора. Под прерыванием при этом понимается любое событие, происходящее в процессе работы КС, которое требует приостановления текущей выполняемой программы для его обработки компьютерной системой, например, нажатие клавиши на клавиатуре или нажатие кнопки мыши, поступление запроса на ввод или вывод данных и т.д.

При возникновении любого прерывания активизируется следующая последовательность действий:

1. выполняемая процессором программа останавливается;
2. осуществляется сохранение информации о текущем состоянии процессора, куда входит и информация о адресе оперативной памяти, по которому находится следующая команда прерванной программы;
3. из таблицы векторов прерываний (таблицы адресов программ обработки прерываний) выбирается адрес программы обработки возникшего прерывания;
4. управление передается программе обработки по выбранному адресу оперативной памяти;
5. после окончания программы обработки прерывания на основе сохраненной ранее информации восстанавливается состояние центрального процессора, которое было в момент возникновения прерывания, и прерванная программа продолжает свое выполнение.

Под вектором прерывания понимается совокупность идентификатора типа прерывания, а также соответствующего ему адреса программы его обработки. Таблица же векторов прерываний, хранящаяся в оперативной памяти, представляет собой список однотипных элементов, в качестве каждого из которых выступает вектор прерывания.

Для контроля доступа к заданному ресурсу необходимо:

1. определить адрес в таблице векторов прерываний, который соответствует обработчику прерывания, активизируемому ОС для доступа к контролируемому ресурсу;
2. подменить найденный адрес на адрес программы контроля санкционированности доступа;
3. вставить перед окончанием программы контроля команды, которые должны:
    - ♦ передать управление стандартному обработчику подмененного прерывания только в том случае, если запрос пользователя на доступ к ресурсу соответствует его полномочиям;
    - ♦ в случае несоответствия запроса пользовательским полномочиям активизировать программу реакции на попытку несанкционированного доступа.

Подмена адресов векторов прерываний выполняется с помощью специально разработанной программы, запускаемой в процессе загрузки ОС. Перед запуском программы подмены адресов обработчиков прерываний должна быть запущена программа идентификации и аутентификации пользователя. Поэтому, может использоваться вариант, когда управление программе подмены адресов обработчиков передается непосредственно из программы идентификации и аутентификации пользователя.

Запуск любой подсистемы защиты (программы идентификации и аутентификации, программы подмены адресов обработчиков прерываний или антивирусной программы) в процессе загрузки ОС может быть выполнен одним из следующих способов:

- ♦ путем использования главного загрузочного сектора винчестера или загрузочного сектора активного раздела жесткого диска;
- ♦ путем указания необходимости запуска соответствующей подсистемы защиты в файлах конфигурирования и настройки ОС, используемых в процессе ее загрузки, например, в файлах CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI или в системном реестре ОС Windows.

Для запуска подсистемы защиты с использованием главного загрузочного сектора винчестера или загрузочного сектора активного раздела жесткого диска в соответствующую область винчестера записывается загрузчик подсистемы защиты. Загружаемая же с помощью этого загрузчика программа по окончании своей работы, в случае принятия решения о продолжении загрузки ОС, должна выполнить функции подмененного загрузчика или передать ему управление.

При указании необходимости запуска соответствующей подсистемы защиты в файлах конфигурирования и настройки ОС следует позаботиться о том, чтобы злоумышленник не смог блокировать загрузку соответствующего программного компонента или, чтобы вероятное блокирование было

бесполезным по причине невозможности последующего доступа к защищаемым ресурсам.

Если при разработке подсистемы разграничения возникают сложности с программной реализацией функции контроля запуска программ, то следует помнить, что выполнение данной функции можно осуществить и за счет разграничения доступа к элементам файловой структуры. По отношению к конкретному пользователю в этом случае для всех программ, запуск которых ему запрещен, должен устанавливаться режим недоступности соответствующих файлов.

Из вышесказанного становится понятным, что для разработки подсистемы разграничения доступа, а также большинства других компонентов системы защиты необходимо детальное знание всех системных соглашений, положенных в основу работы используемой ОС. В ряде случаев эти соглашения могут быть получены только у разработчика операционной системы.

7 Реализация криптографического закрытия конфиденциальных данных в «Secret Net 5.1»

Для обеспечения надежного контроля доступа к ресурсам компьютера необходимо такое построение ОС, чтобы доступ со стороны прикладных программ к этим ресурсам был возможен только через доступ к функциям операционной системы. При этом любой запрос со стороны прикладной программы на доступ к какому-либо ресурсу КС должен удовлетворяться системой защиты только при наличии у пользователя, от имени которого выполняется данная прикладная программа, соответствующих полномочий.

К сожалению, не все ОС ограничивают возможность доступа к ресурсам КС только доступом через обращение к функциям операционной системы. Операционные системы Windows позволяют осуществить доступ к компьютерным ресурсам в обход предоставляемого ими программного интерфейса. При этом для прикладных программ возможны следующие пути обхода контролируемых функций этих операционных систем:

- ♦ использование прерываний базовой системы ввода-вывода (BIOS);
- ♦ непосредственное использование функций BIOS по их адресам во внутренней памяти компьютера;
- ♦ доступ к ресурсу на уровне контроллера внешнего устройства.

Учитывая наличие путей обхода можно сделать вывод, что для обеспечения высокого уровня информационной безопасности подсистема разграничения в этих ОС должна иметь возможность криптографического закрытия конфиденциальных данных. В этом случае, даже при условии блокирования или обхода злоумышленником уровня контроля установленных полномочий, получить конфиденциальную информацию будет невозможно по причине того, что она зашифрована.

Именно такая стратегия разграничения доступа реализована, например, в системе защиты «Secret Net 5.1». В данной системе управление шифрованием файлов и доступом к ним осуществляется на уровне каталога. Поэтому каталог, в котором размещаются зашифрованные файлы, называют «шифрованный каталог» или «шифрованный ресурс».

Пользователь, создавший шифрованный ресурс, является его владельцем и может предоставлять доступ к ресурсу другим пользователям, а также делегировать им полномочия на управление шифрованным ресурсом. Пользователь ресурса может создавать новые зашифрованные файлы, удалять их, выполнять с ними любые операции чтения и записи.

Управляющая структура шифрованного каталога сохраняется в отдельном скрытом файле !Res.key, который помещается в этот каталог. Это позволяет шифровать ресурсы на различных файловых системах (FAT, NTFS).

Генерация ключей пользователей осуществляется в соответствии с требованиями ГОСТ Р34.10-2001. Для пользователя создается ключевая пара,

состоящая из закрытого и открытого ключей. Открытый ключ пользователя хранится в локальной базе данных «Secret Net 5.1», закрытый ключ – в персональном идентификаторе пользователя.

После смены ключей пользователя в системе хранятся две ключевые пары – текущая и предыдущая. Предыдущая ключевая пара необходима для перешифрования на новом ключе управляющей информации шифрованных ресурсов пользователя. Процесс перешифрования управляющей информации запускается автоматически после смены ключей. Для обеспечения своевременной замены ключей можно установить минимальное и максимальное время жизни ключевой пары.

При смене ключей пользователя заново зашифровывается только управляющая информация шифрованных ресурсов. Сами данные (шифрованные файлы) не перешифровываются. При необходимости перешифрования файлов шифрованного ресурса следует создать новый шифрованный ресурс.

Общие сведения о ключевой схеме в системе защиты «Secret Net 5.1»:

При шифровании данных используются следующие ключи:

Ключ	Наименование	Алгоритм генерации
SKr	Закрытый ключ ресурса	Генерируется в соответствии с ГОСТ Р34.10-2001
PKr	Открытый ключ ресурса (соответствует закрытому ключу SKr)	– " –
SKu	Закрытый ключ пользователя	– " –
PKu	Открытый ключ пользователя (соответствует закрытому ключу SKu)	– " –
Kr	Ключ шифрования ресурса	Генерируется с помощью датчика случайных чисел (ДСЧ) в соответствии с ГОСТ 28147-89
Kf	Ключ шифрования файла	– " –
SKur	Сессионный ключ. Может быть получен из пары ключей SKu и PKr или SKr и PKu	Генерируется в соответствии с алгоритмом Diffie-Hellman

На следующем рисунке представлена схематическая иллюстрация использования ключей:

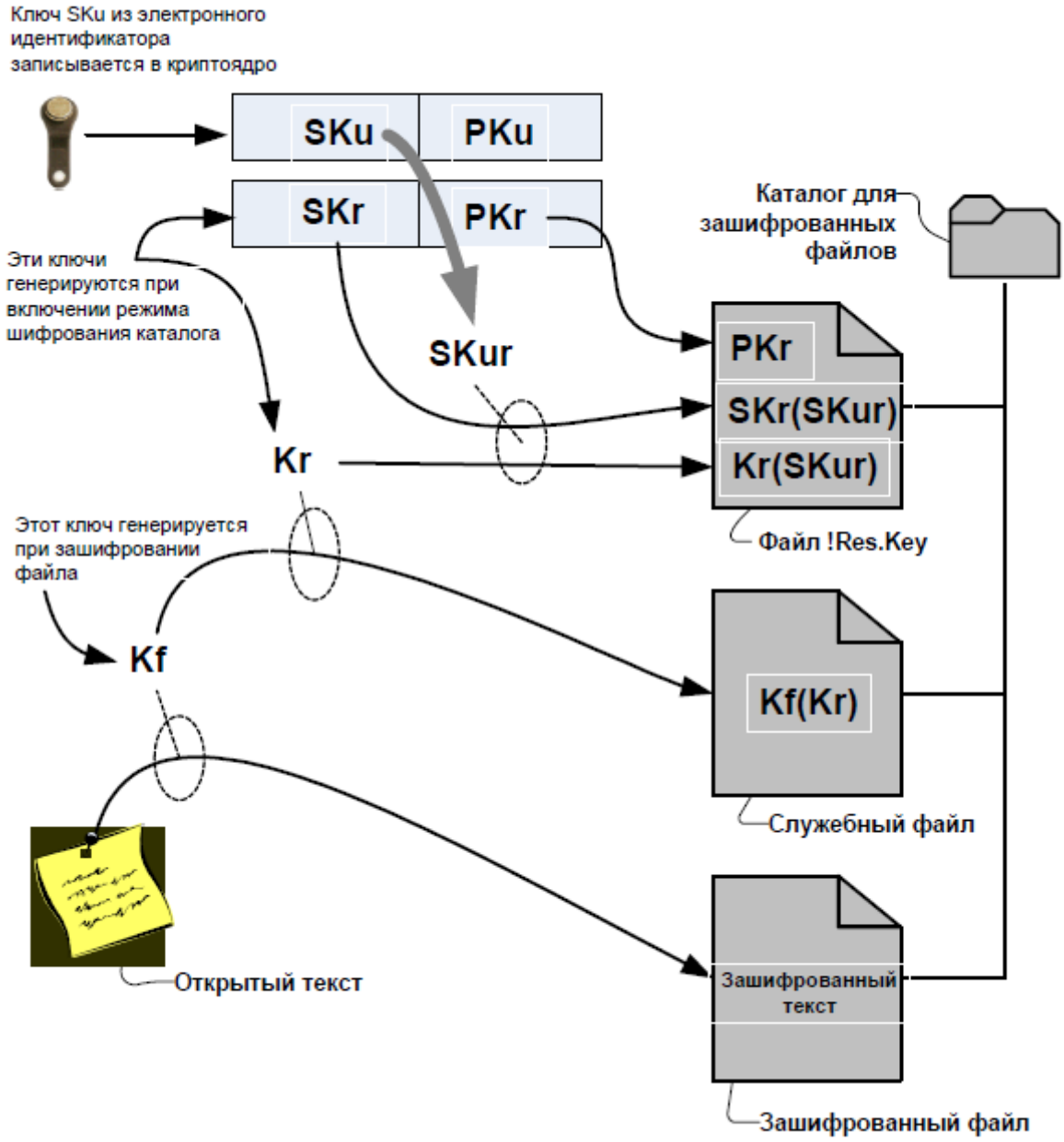


Рисунок 5. Схема использования ключей в системе защиты «Secret Net 5.1»

В системе «Secret Net 5.1» предусмотрена также возможность ограничения доступа пользователей к съемным устройствам (в том числе USB-накопителям). Включение режима ограничения осуществляется заданием администратором режима контроля аппаратных устройств. В этом случае будет осуществляться проверка аппаратной конфигурации при загрузке ПЭВМ и в процессе ее работы. При подключении незарегистрированного аппаратного устройства произойдет блокировка ПЭВМ, разблокировать сможет только администратор безопасности. В

результате станет возможна работа только с теми устройствами, которые специально зарегистрированы администратором безопасности.

Следует отметить, что если задача разграничения доступа пользователей к компьютерным ресурсам является особенно актуальной и КС основана на высокопроизводительной аппаратной базе, то для эффективного контроля установленных полномочий пользователей целесообразно использование операционных систем, имеющих встроенные средства разграничения, например – МС ВС 3.0, либо использовать наложенные средства защиты информации.

ЗАКЛЮЧЕНИЕ

В результате изучения данного учебно-методического пособия и выполнения лабораторной работы «Система защиты информации Secret Net 6.0» студенты получают знания основных подходов управления доступом к информационным ресурсам, умения анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач, а также приобретают навыки использования современных программно-аппаратных средств защиты информации. Знания, полученные при изучении системы защиты информации (СЗИ) Secret Net 6.0, помогут в дальнейшем освоить любые другие СЗИ.

Перечень компетенций, формируемых у студента в ходе освоения дисциплины «Программно-аппаратная защита информации»:

В области знания и понимания:

- знает основные подходы к защите данных от НСД;
- знает методы и средства ограничения доступа к компонентам ЭВМ;
- знает необходимые и достаточные функции аппаратного средства криптозащиты;
- знает необходимые и достаточные условия недопущения разрушающего воздействия;
- знает наиболее уязвимые для атак противника элементы компьютерных систем.

В области интеллектуальных навыков:

- владеет механизмами решения типовых задач защиты информации;
- владеет технологиями формирования изолированной программной среды;
- владеет технологиями защиты программ от несанкционированного копирования;
- владеет технологиями защиты программ от разрушающих программных воздействий.

В области практических навыков:

- умеет анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач;
- умеет применять штатные средства защиты и специализированные продукты для решения типовых задач;
- умеет квалифицированно оценивать область применения конкретных механизмов защиты;
- умеет грамотно использовать аппаратные средства защиты при решении практических задач.

В области переносимых навыков:

- ориентируется в продуктах и тенденциях развития средств защиты информационных технологий;

- доказывает корректность использования полученных навыков в применении к задачам защиты информации с использованием программно-аппаратных средств защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: учеб. пособие – Владивосток: Изд-во ДВГТУ, 2007. – 318 с.
2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.: Агентство «Яхтсмен», 1996.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000.
4. Стахнов А. А. Linux: 3-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2009. – 1056 с.
5. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: ГТК, 1992.
6. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М.: ГТК, 1992.
7. www.securitycode.ru
8. www.fstec.ru

ПРИЛОЖЕНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНОЙ РАБОТЕ ПО ДИСЦИПЛИНЕ ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ

Лабораторная работа.
Система защиты информации Secret Net 6.0

Цель работы: Изучить систему защиты информации (СЗИ) Secret Net 6.0 для обеспечения информационной безопасности в локальной вычислительной сети.

Теоретические сведения

Назначение:

Система Secret Net 6.0 предназначена для предотвращения несанкционированного доступа к рабочим станциям и серверам, работающим в гетерогенных локальных вычислительных сетях под управлением ОС MS Windows 2000, MS Windows XP, MS Windows Vista, MS Windows 7, MS Windows Server 2003 и MS Windows Server 2008.

Secret Net 6.0 дополняет своими защитными механизмами стандартные защитные средства операционных систем и тем самым повышает защищенность всей автоматизированной информационной системы предприятия в целом, обеспечивая решение следующих задач:

- управление правами доступа и контроль доступа субъектов к защищаемым информационным, программным и аппаратным ресурсам;
- управление доступом к конфиденциальной информации, основанное на категориях конфиденциальности;
- шифрование файлов, хранящихся на дисках;
- контроль целостности данных;
- контроль аппаратной конфигурации;
- дискреционное управление доступом к устройствам компьютера;
- регистрация и учет событий, связанных с информационной безопасностью;
- мониторинг состояния автоматизированной информационной системы;
- ролевое разделение полномочий пользователей;
- аудит действий пользователей (в том числе администраторов и аудиторов);
- временная блокировка работы компьютеров;
- затирание остаточной информации на локальных дисках компьютера.

Функциональные части Secret Net 6.0

Система Secret Net 6.0 состоит из трех функциональных частей:

- защитные механизмы, которые устанавливаются на все защищаемые компьютеры автоматизированной системы (АС) и представляют собой

набор дополнительных защитных средств, расширяющих средства безопасности ОС Windows.

- средства управления защитными механизмами, которые обеспечивают централизованное и локальное управление системой.
- средства оперативного управления, которые выполняют оперативный контроль (мониторинг, управление) рабочими станциями, а также централизованный сбор, хранение и архивирование системных журналов.

Администратору безопасности предоставляется единое средство управления всеми защитными механизмами, позволяющее централизованно управлять и контролировать исполнение требований политики безопасности.

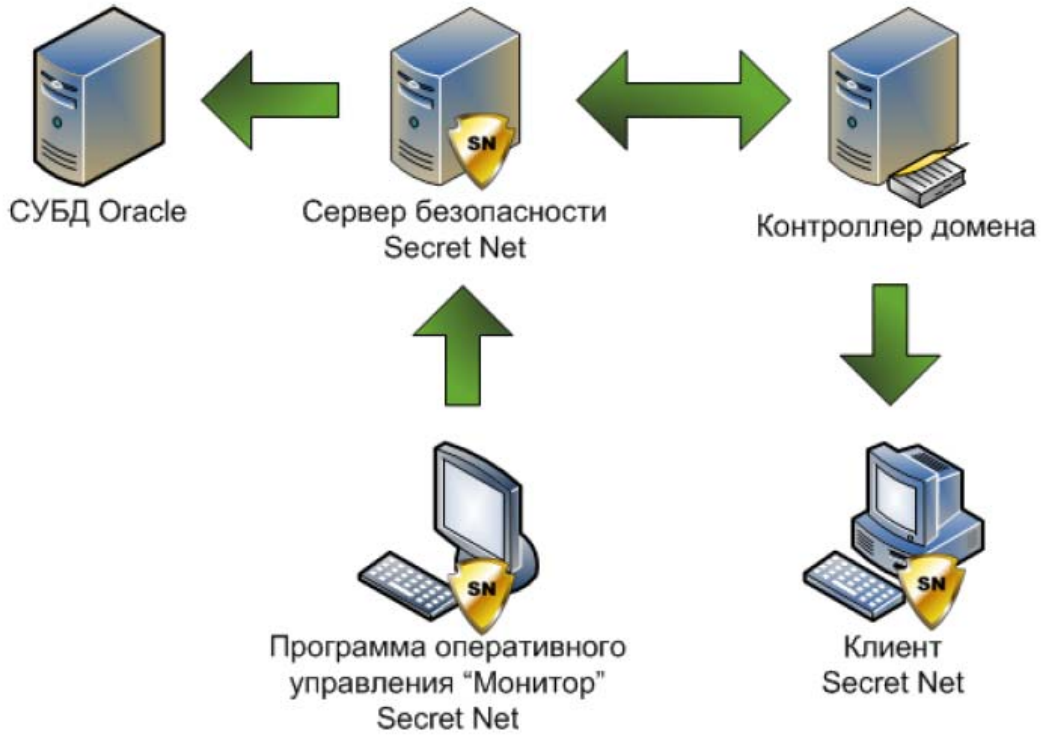
Вся информация о событиях в информационной системе, имеющих отношение к безопасности, регистрируется в едином журнале регистрации. О попытках свершения пользователями неправомерных действий администратор безопасности узнает немедленно.

Существуют средства генерации отчетов, предварительной обработки журналов регистрации, оперативного управления удаленными рабочими станциями.

Компоненты Secret Net 6.0

Secret Net 6.0 состоит из трёх компонентов:

1. СЗИ Secret Net 6.0 – Клиент. Устанавливается на все защищаемые компьютеры. В состав этого ПО входят следующие компоненты:
   - Защитные механизмы – совокупность настраиваемых программных и аппаратных средств, обеспечивающих защиту информационных ресурсов компьютера от несанкционированного доступа, злонамеренного или непреднамеренного воздействия.
   - Модуль применения групповых политик.
   - Агент сервера безопасности.
   - Средства локального управления – это штатные возможности операционной системы, дополненные средствами Secret Net 6.0 для управления работой компьютера и его пользователей, а также для настройки защитных механизмов.
2. СЗИ Secret Net 6.0 – Сервер безопасности. Включает в себя:
   - Собственно сервер безопасности.
   - Средства работы с базой данных (БД).
3. СЗИ Secret Net 6.0 – Средства управления. Включает в себя:
   - Программу «Монитор». Эта программа устанавливается на рабочем месте администратора оперативного управления – сотрудника, уполномоченного контролировать и оперативно корректировать состояние защищаемых компьютеров в режиме реального времени.



Особенностью системы Secret Net 6.0 является клиент-серверная архитектура, при которой серверная часть обеспечивает централизованное хранение и обработку данных системы защиты, а клиентская часть обеспечивает защиту ресурсов рабочей станции или сервера и хранение управляющей информации в собственной базе данных.

Клиентская часть системы защиты

Клиент Secret Net 6.0 (как автономный вариант, так и сетевой) устанавливается на компьютер, содержащий важную информацию, будь то рабочая станция в сети или какой-либо сервер (в том числе и сервер безопасности).

Основное назначение клиента Secret Net 6.0:

Защита ресурсов компьютера от несанкционированного доступа и разграничение прав зарегистрированных пользователей. Регистрация событий, происходящих на рабочей станции или сервере сети, и передача информации на сервер безопасности. Выполнение централизованных и децентрализованных управляющих воздействий администратора безопасности.

Клиенты Secret Net 6.0 оснащаются средствами аппаратной поддержки (для идентификации пользователей по электронным идентификаторам и управления загрузкой с внешних носителей):

- программно-аппаратный комплекс «Соболь»;
- плата Secret Net Touch Memory Card 2.

В качестве индивидуальных идентификаторов могут быть использованы:

- iButton (серия DS199x);
- eToken;
- USB флэш диск.

Сервер безопасности

Сервер безопасности устанавливается на выделенный компьютер или контроллер домена и обеспечивает решение следующих задач:

- Ведение центральной базы данных (ЦБД) системы защиты, функционирующую под управлением СУБД Oracle 9.2 Personal Edition и содержащую информацию, необходимую для работы системы защиты.
- Сбор информации о происходящих событиях со всех клиентов Secret Net 6.0 в единый журнал регистрации и передача обработанной информации подсистеме управления.
- Взаимодействие с подсистемой управления и передача управляющих команд администратора на клиентскую часть системы защиты.

Подсистема управления Secret Net 6.0

Подсистема управления Secret Net 6.0 устанавливается на рабочем месте администратора безопасности и предоставляет ему следующие

возможности: Централизованное управление защитными механизмами клиентов Secret Net 6.0. Контроль всех событий имеющих отношение к безопасности информационной системы. Контроль действий сотрудников в информационной системе организации и оперативное реагирование на факты и попытки НСД. Планирование запуска процедур копирования ЦБД и архивирования журналов регистрации. Схема управления, реализованная в Secret Net 6.0, позволяет управлять информационной безопасностью в терминах реальной предметной области и в полной мере обеспечить жесткое разделение полномочий администратора сети и администратора безопасности.

Автономный и сетевой вариант

Система защиты информации Secret Net 6.0 выпускается в автономном и сетевом вариантах.

Автономный вариант - состоит только из клиентской части Secret Net 6.0 и предназначен для обеспечения защиты автономных компьютеров или рабочих станций и серверов сети, содержащих важную информацию.

Сетевой вариант - состоит из клиентской части, подсистемы управления, сервера безопасности и позволяет реализовать защиту, как всех компьютеров сети, так и только тех рабочих станций и серверов, которые хранят и обрабатывают важную информацию. Причем в сетевом варианте, благодаря наличию сервера безопасности и подсистемы управления, будет обеспечено централизованное управление и контроль работы всех компьютеров, на которых установлены клиенты Secret Net 6.0.

Сферы применения Secret Net 6.0

Основными сферами применения системы Secret Net 6.0 являются:

- защита информационных ресурсов;
- централизованное управление информационной безопасностью;
- контроль состояния информационной безопасности.

Порядок выполнения работы

1. Ознакомиться с системой защитой информации Secret Net 6.0.
2. Установить систему защиты информации Secret Net 6.0 на ПЭВМ и просмотреть настройки данной системы.
3. Исследовать возможные механизмы, обеспечивающие защиту и безопасность рабочих станций и серверов сети.
4. Описать структурную схему системы Secret Net 6.0, в которую входят:

- клиентская часть;
- сервер безопасности;
- подсистема управления.

5. Обосновать технические характеристики программно-аппаратного комплекса для обеспечения информационной безопасности в локальной вычислительной сети на базе Secret Net 6.0.

Содержание отчета

1. Теоретические сведения.
2. Полное описание компонент системы Secret Net 6.0.
3. Примеры автономного и сетевого варианта системы Secret Net 6.0.
4. Расчет технических характеристик программно-аппаратного комплекса для обеспечения информационной безопасности в локальной вычислительной сети на базе Secret Net 6.0.
5. Выводы по работе.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы.

КАФЕДРА ПРОЕКТИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

1945-1966 РЛПУ (кафедра радиолокационных приборов и устройств). Решением Советского правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения. Приказом по институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Название кафедры в тот период открыто не упоминалось, а она имела номер 11.

Организатором и первым заведующим кафедрой до 1951 г. был д.т.н., профессор С. И. Зилитинкевич, который являлся крупнейшим деятелем в области радиотехники и электроники, автором ряда важнейших исследований и открытий.

В течение первого года своего существования кафедра развивалась чрезвычайно быстро. Основной лабораторной базой в то время были радиолокационные станции типа «Вюрсбург» (снятая с немецкого поезда) и первая отечественная станция типа «Пегматит». Лишь в пятидесятые годы появились на кафедре действующие отечественные станции «Мист-2», «Кобальт», «П-8» и ряд других.

С 1951 года по 1954 кафедру возглавлял крупный специалист в области передающих устройств РЛС, один из ведущих работников радиопромышленности, кандидат технических наук, доцент А.И. Лебедев-Карманов (по совместительству).

На кафедре № 11 проводилась также большая научно-исследовательская работа. Так, в 1952-1953 годах по заказу Военно-медицинской академии был разработан и изготовлен первый отечественный электокардиограф.

В 1954 году А.А. Тудоровский, ставший к этому времени доцентом, был избран заведующим кафедры № 11. Постепенно состав кафедры начал пополняться се молодыми выпускниками. Одновременно на кафедру поступило новое оборудование, в том числе современная измерительная аппаратура, что позволило создать собственную лабораторную базу по всем курсам.

Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. – радиоинженер (специальность 0705).

В 1970 году радиотехнический факультет ЛИТМО был ликвидирован. Кафедру КиПРЭА переименовали в кафедру «Конструирования и производства электронно-вычислительной аппаратуры» (КиПЭВА) и перевели на факультет точной механики и вычислительной техники. Коренной переделке подвергся учебный план, по которому велась подготовка специалистов. Были выделены два основных направления: автоматизация конструирования ЭВА и технология производства микроэлектронных устройств ЭВА. Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско–технологической направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер–конструктор–технолог РЭА.

Заведовал кафедрой доцент А.Н. Иванов.

В конце 1973 года на должность заведующего был избран д.т.н. профессор Ф.Г.Старос. Профессор Ф.Г.Старос являлся одним из основных родоначальников отечественной микроэлектроники. Он был главным разработчиком Советского центра микроэлектроники в Зеленограде. Под его руководством был разработан и изготовлен первым в мировой практике прообраз персонального компьютера - УМ-1-НХ. В связи с назначением профессора Ф.Г.Староса директором одного из институтов АН СССР во Владивостоке в начале 1974 года, он вынужден был оставить кафедру КиПЭВА. В это время на должность заведующего кафедрой был избран выпускник ЛИТМО 1959 года к.т.н. доцент В.В.Новиков (впоследствии д.т.н., профессор). С приходом В.В.Новикова резко усилилась работа в области микроэлектроники. Были открыты научно-исследовательские темы по применению новых физических принципов при разработке различных электронных устройств. Большое участие в этих разработках принимали доценты А.В.Панков и В.С Салтыков.

С 1976 по 1996 кафедрой руководил известный специалист в области автоматизации проектирования электронных устройств профессор

Г.А.Петухов (с небольшим перерывом, когда с 1988 по 1992 год кафедру возглавлял ученик Г.А.Петухова профессор С.А.Арустамов, который в дальнейшем ушел из ЛИТМО, в связи с переходом на другую работу). За это время получило дальнейшее направление развитие автоматизации проектирования. Был создан один из первых в ЛИТМО собственный машинный класс. Научная работа была в основном сконцентрирована в области САПР. Так в это время на кафедре проводилась большая научно-исследовательская работа по автоматизации топологического проектирования БИС на базовых кристаллах, которую возглавляли профессора Г.А. Петухов и С.А. Арустамов.

С 1996 года кафедру возглавляет ее воспитанник д.т.н., профессор Ю.А.Гатчин. Помимо традиционной подготовки инженеров конструкторов-технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205), была начата подготовка специалистов по специальности 090104 «Комплексная защита объектов информатизации», причем основное внимание уделяется программно-аппаратной защите информации компьютерных систем.

В 1998 году кафедра была переименована и получила название «Кафедра проектирования компьютерных систем», что отразило содержание основных научных исследований и направления подготовки студентов и аспирантов.

За время своего существования кафедра выпустила более 4500 дипломированных инженеров. Более 50 молодых ученых защитили кандидатские диссертации, 10 человек защитили диссертации на соискание ученой степени доктора технических наук.