Защита компьютерной информации

Михальцов П.А.

1 февраля 2020 г.

1 Защита информации в информационно вычислительных системах

1.1 Проблемы защиты компьютерной информации

Вопросы

1. Основное понятия об угрозах информационной безопасности
2. Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации
3. Задачи информационной безопасности

1.1.1 Основное понятия об угрозах информационной безопасности

Информационная безопасность — такое состояние системы, при которой она может противостоять против дестабилизирующий воздействию внешних и внутрений угроз, а также – её функционирования не создаёт информационных угроз для элементов самой системы и внешней среды

Обеспечение информационной безопасности проблемы может быть достигнуто лишь при взаимоувязанном решении трёх составляющих проблем:

- защита находящееся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации
- защита элементов системы от дестабилизирующий воздействия внешних и внутренних информационных угроз

- защита внешний среды от информационной угроз со стороны рассматриваемой системы

Под ***защитой информации*** понимать совокупность мероприятий и действий, направленнох на обеспечение её безопасности – конфендициальность и целосность – в процессе сбора, перердачи, обработки и хранения.

Безопасностъ информациии - это свойство (состояние) передаваемой накапливаемой, обрабатываемой и хранимой информации, характеризующие её степень защищенности от дистабилизирующиго воздействия внешней среды и внутренних угроз то есть её конфендициальность, сигнальная скрытность(энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующими и искажающим воздействиям и помехам.

Под ***защитой информации*** в более широком смысле понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Защита информации направлена на:

- предупреждение угроз как превентивных мер по обеспечению безопасности в интересах учреждения возможности их возникновения.
- выявление угроз, которое выражается в систематическом анализе и контроле возможности появления реальных и потенциальных угроз и своевременных мер по их предупреждению.
- обнаружение угроз, целью которого является определение реальных угрозы или конкретных преступных деятельности.
- ликвидацию последствий угроз и преступных действий и восстановления статуса-кво.

Обнаружение угроз — это действие по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба.

Пресечение или локализация угроз — это действие, направленное на устранение действующей угрозы и конкретных преступных действий

Ликвидация последствий имеет целью восстановлению состояния, предшествовавшего наступлению угрозы.

1.1.2 Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации

Актуальность и важность информационной безопасности(ИБ) обусловленна следующими факторами:

- высокие темпы роста парка ПК, применимых в разных сферах деятельности, и как следствие, резкое расширение круга пользователей, имеющих непосредственный доствуп к вычислительным сетям и информационным ресурсам.
- увеличение объеммов информации с помощью ПК и др. средств автоматизации
- бурное развитие апаратно–программных средств и технологий не удовлетворяющих современных ТБ.
- несоответствию развития средств обработки информации и проработки теорий ИБ разработки международных стандартов и правовых норм, обеспечивающих необходимый уровень ЗИ защиты информации
- повсеместное распространения сетевых технологиой, создание единого информационно-коммуникативной сети Интернет, которая не может обеспечить достойного уровня ИБ.

Цели защиты ифформации являются

- предотвращения утечи хищения утраты искажения поделки информации
- предоствращение угроз безопасности личности, общества, гос–ва.
- предотвращение ненксанционированного действий по уничтожению, модификации, искажению, кописрования, блокировки информации.
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы
- обеспечение правого режима документированной информации как объекта собственности
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах

- сохранение государственной тайны документированной информации в соответствии с законодательством
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения

1.1.3 Задачи информационной безопасности

Основные задачи системы ИБ является

- своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующей нанесению финансовой или другого ущерба.
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия.
- эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и техническим мер и средств обеспечения безопасности
- Создание условий для возмещения м локализации нанесённого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушений безопасности на достижение целий организаций

1.2 Угрозы безопасности в информационно вычислительных системах

Вопросы

- Понятия угрозы безопасности
- Актуальность проблемы обеспечение информационной безопасности
- Задачи защиты информации
- Задачи информационной безопасности

Угроза — это потенциальное возможная событие, действия(воздействия), процесс или явления которые может провести к нанесению ущерба чьим либо интересам.

Существуют три разновидности угроз

- Угрозы нарушения конффендициальности
- Угрозы нанесения целостности
- Угрозы отказа служб

Угроза нарушения конфендициальности — информация становится известна тому кто не располагает полномочий к ней

Угроза нарушения целостности — заключает в себе любое умышленное изменение информации хранящая в себе(вычислительной системы) или передаваемой из одной системы в другую.

Угроза отказа служб — когда в результате преднамеренных действий предпринимаемый другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

Доступность информации — это свойство системы (среды, средств и технологий обработки) в которой циркулирует информация харктерезующая способность обеспечивать своевременную беспрепятственный доступ субъектов к интересующих их информации и готовность соответствующему автоматизированных служб к обслуживанию от субъектов запросов всегда, когда в обращении к ним.

Классификация угроз информационной безопасности

- По природе возникновения
- По степени предномерености появления

1. появление ошибок в программно-апаратных средств АС
2. некомпетентное использование или настройка или неправомерное средств защиты персоналом службы безопасности
3. неумышленное действие, приводящая к частичному или полному отказу системы или разрушения апоратных, программынх, информационных ресурсов системы
4. Неправомерное включение оборудования или изменение режимов работы устройств и программ
5. Неумышленная порча носителей информации
6. Пересылка данных по ошибочному адресу абонента(устройства)
7. Ввод ошибочных данных
8. Неумышленное повреждение каналов связи

- Угрозы преднемерного действия

1. Традиционный или универсальный шпионаж и диверсия.
2. Несанкционированный доступ к информации
3. Несанкционирование модификация структур
4. Информационные инфекции
5.

1.3 Основные направления использования средств и методов защиты информации

1.3.1 Средства и методы обеспечения целостности

Угроза целостности – угроза, в результате реализации которой информация становится изменённой или уничтоженной. Необходимо отметь, что и в нормальном режиме работы АС данные могут изменяться и удаляться.

Методы обеспечения безопасности:

1. Обеспечение отказоустойчивости (резервирование)
2. Обеспечение безопасного восстановление (резервное копирование и электронное архивирование информации)

1.3.2 Средства и методы обеспечения конфиденциальности

1. Разграничение доступа к данным
2. Парольная защита
3. Шифрование
4. Скрытие данных
5. Уничтожение остаточных данных
6. Защита от копирования программных систем

1.3.3 Общая схема процесса обеспечения безопасности

Категории методов защиты от НСД:

1. Организационные
2. Технологические
3. Правовые

Требования для работы с информации 1-го класса:

1. Осведомление сотрудников о закрытости данной информации
2. Общее ознакомление сотрудников с основными возможными методами атак на информацию
3. Ограничение физического доступа
4. Полный набор документации по правилам выполнения операций с данной информацией

Требования для работы с информацией 2-го класса:

1. Расчёт рисков атак на информацию
2. Поддержание списка лиц, имеющих доступ к данной информации
3. По возможности выдача подробной информации под расписку (в т.ч. электронной)
4. Автоматическая система проверки целостности системы и её средств безопасности

Уровень доступа к информации в АС	Основные методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза отказа служб (отказа доступа к информации)
Носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации. Перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Средства взаимодействия с носителей	Получение информации о программно-аппаратной среде. Получение детальной информации о функциях, выполняемы АС. Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам АС. Совершение пользователем несанкционированных действий. Несанкционированное копирование ПО. Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные. Установка и использование нештатного ПО. Заражение программными вирусами.	Проявление ошибок проектирования и разработки программно-аппаратных компонентов АС. Обход механизмов АС.
Представления информации	Определение способа представления информации	Визуальное наблюдение. Раскрытие представления информации (дешифрование)	Внесение искажения в представление данных; уничтожение данных	Искажение соответствия синтаксических и сематических конструкций языка
Содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержание информации	Внедрение дезинформации	Запрет на использование информации

Рис. 1:

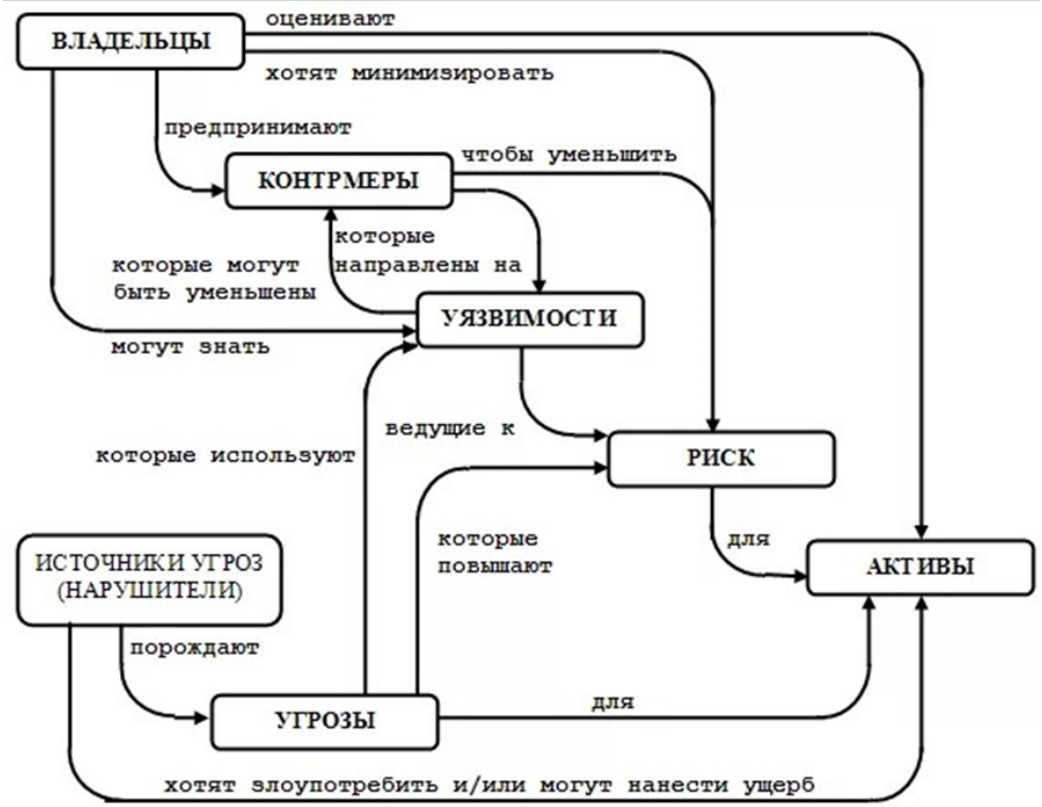

Рис. 2:

5. Надёжные схемы физической транспортировки
6. Обязательное шифрование при передаче по линиям связи
7. Схема бесперебойного питания ЭВМ

Требования для работы с информацией 3-го класса:

1. Детальный план спасения либо надёжного уничтожения информации в аварийных ситуациях (пожар, наводнение, взрыв)
2. Защита ЭВМ либо носителей информации от повреждения водой и высокой температурой
3. Криптографическая проверка целостности информации

2 Правовые и организационные методы защиты информациии в информационно вычислительных системах

2.1 Стандарты и спецификации в области информационной безопасности

Вопросы

1. Стандарт ISO 15408 "Критерии оценки безопасности технологий"
2. критерии оценки надёжных компьютерных систем

2.1.1 Стандарт ISO 15408 "Критерии оценки безопасности технологий"

Стандарт ISO 15408 принят 1 декабря 1999 часто называется Общие критерии (ОК)

Характиристика угроз :

1. источник угроз
2. методы воздействия
3. уязвимыми местами которые могут быть использованы
4. ресурсы которые могут пострадать

Уязвимые места возникают тогда

1. требования безопасности
2. проектирование
3. эксплуатация

2 основные требования безопасности стандарт ISO 15408:

1. Функциональные, соотведстует активному аспекту зациты предьявляемой к функцим безопасности и реализующим их механизмам
2. Требования доверия, СООТВЕДСТВУЮЩИЕ ПАССИВНОМУ АСПЕКТУ.

Классы функциональных требований ОК:

1. Индификация и аутодификация
2. защата данных пользователя
3. приватность
4. использование ресурсов
5. крипрографическая подержка

Форма предоставления теребований доверия принцепи не чем не отличается от функциональным, отличие что кажждое действие пренаждлежит одному типу:

1. действия разработчиков
2. предоставление и содержание свидетельства
3. действия оценщиков

Классы требований доверия безопасности ОК:

1. Разработка
2. подержка ЖЦ
3. тестирование
4. оценка уязвимости
5. поставка и эксплуатация
6. упровление конфигурацией
7. руковонство
8. поддержка доверия
9. оценка профиля защиты
10. оценка задания по безопасности

В ОК введене оценочные уровни (7 штук):

1. Оценочный уровень доверия 1. Анализ функциональных спецификаций, специальных интерфейсов, а текже независемое тестирование. Урове нь применим, когда угрозы не рассматириваются как сериёзные

2. Оценочный уровень доверия 2. Предусматривает наличие проекта верхнего уровня объекта оценки выборочное тестирование, анализ стойкости функции безопасности, поиск разработчиком явных уязвимых мест.

3. Оценочный уровень доверия 3.Ведётся контроль среды разработки и упровления конфигурацией объектов оценки.

4. Оценочный уровень доверия 4. Полная спецификация интерфейсов, проектов нижнего уровня, анализ подмножества реализации, применение неформальный модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией.

5. Оценочный уровень доверия 5. в дополнение к предудущим предусматривает применение формальцной модели политика политики безопасности полуформальных функциональноной спецификации и проекта. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

6. Оценочный уровень доверия 6. Реализация должна быть представленна в структурном види. Анализ соотведствия распостраняется на проект нижнего уровня

7. Оценочный уровень доверия 7. Предусматривает формальныую вирификацию проекта обхекта оценки. Он применим к ситуациям черезвычайно высогого риска.

2.1.2 Критерии оценки надёжных компьютерных систем

Степень доверия или надежность систем, оценивается по двум основным критериям

1. Политика безопасности - набор законов, правил норм поведения, определяющих, как организация обрабатывает, защищает и распостраняет информцию.

2. Гарантированость — мера доверия, которая может быть оказана архетектуре и реализации системы. Гарантированность может происходить как из тестирования, так и из проверки общего замысла и исполннение системы в целом и её компонентов.

3. Надажнось вычислительная база — это совокупность защатных механизмов компьютерной системы, отвечающих за проведение в жизни политики безопасности

4. Основное назначение надежной вычислительной базы — выполнит финкции монитора обращений, то есть контролировать доступность выполнения субъектами определеных операций нал объектами.

От монитора обращение требуется выполнение трех свойств:

1. Изолированость. Монитор должен быть защащен от отслуживания свией работы.

2. Полнота. Монитор должен вызывать при каждом обращении не должно быть способов его обхода

3. Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестировании.

Основыне элементы политики безоасности

1. произволоное упровление доступом

2. безопасность повторного использование объектов

3. метки безопасности

4. принудительное упровление доступом

3 Методы идентификации и аутентификации

3.1 Идентификация и аутентификация

3.1.1 Требования к идентификации и аутентификации

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Такую информацию называют идентификатором субъекта. Имея идентификатор, зарегистрированный в сети пользователь считается легальным (заданным); остальные субъекты относятся к нелегальным.

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает две стадии идентификацию и аутентификацию.

Идентификация — это процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Он сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация — процедура проверки подлинности, позволяющая достоверно убедиться, что пользователь является именно тем, кем он себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны; при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация — взаимосвязанные процессы распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу.

3.1.2 Авторизация с точки зрения количества и вида зарегистрированных пользователей

Авторизация – предоставление прав (или привилегий), позволяющих владельцу иметь законный доступ к системе или к её объектам. Механизм авторизации часто называют подсистемой управления доступом, которая также требует проектирования. Процесс авторизации включает в себя идентификацию и аутентификацию пользователей.

В системе зарегистрирован один пользователь

Данный пользователь является и прикладным пользователем, и администратором безопасности. Здесь источником потенциальной угрозы является только сторонний сотрудник предприятия, а вся задача защиты сводится к контролю доступа в компьютер (либо в систему), т.е. к парольной защите.

Данный случай является вырожденным и нами далее не рассматривается, т.к. в соответствии с формализованными требованиями к защите информации от НСД даже при защите конфиденциальной информации предполагается обязательное наличие администратора безопасности.

В системе зарегистрированы администратор безопасности и один прикладной пользователь

Общий случай функционирования системы с одним прикладным пользователем – это наличие в системе администратора безопасности и только одного прикладного пользователя. В задачи администратора безопас-

ности здесь входит ограничение прав прикладного пользователя по доступу к системным (администратора безопасности) и иным ресурсам компьютера. В частности, может ограничиваться набор задач, разрешенных для решения на компьютере, набор устройств, которые могут быть подключены к компьютеру (например, внешний модем, принтер и т.д.), способ сохранения обрабатываемых данных (например, на дискетах только в шифрованном виде) и т.д.

В данном случае потенциальным злоумышленником в части несанкционированного использования ресурсов защищаемого объекта может являться как сторонний сотрудник предприятия, так и собственно прикладной пользователь. Заметим, что прикладной пользователь здесь может выступать в роли сознательного нарушителя, либо стать «инструментом» в роли стороннего нарушителя, например, запустив по чьей-либо просьбе какую-нибудь программу).

В системе зарегистрированы администратор безопасности и несколько прикладных пользователей

Кроме администратора безопасности, в системе может быть заведено несколько прикладных пользователей. При этом ресурсами защищаемого компьютера могут пользоваться несколько сотрудников, решая различные задачи. Ввиду этого информационные и иные ресурсы защищаемого объекта должны между ними разграничиваться.

В данном случае к потенциальным нарушителям добавляется санкционированный прикладной пользователь, целью которого может служить НСД к информации, хранимой на защищаемом объекте другим пользователем.

При использовании компьютера (прежде всего, рабочей станции) в составе ЛВС, помимо локальных ресурсов защищаемого объекта, защите подлежат сетевые ресурсы.

В этом случае между пользователями могут разграничиваться права по доступу к серверам, сетевым службам, разделенным сетевым ресурсам (общим папкам и устройствам, например, к сетевым принтерам) и т.д.

Здесь злоумышленник (санкционированный пользователь) может осуществлять попытку получить НСД к сетевому ресурсу, к которому ему доступ не разрешен, с целью осуществления на него атаки с рабочей станции.

3.1.3 Классификация задач идентификации и аутентификации

Цель идентификации – установить тождественность или подлинность объекта (товара) его основополагающим характеристикам.

На современном этапе задачами идентификации являются:

- определение структуры, норм и правил в области идентификации товаров;

- разработка основополагающих критериев, пригодных для целей идентификации однородных групп, конкретных видов и наименований товаров;

- исследование потребительских свойств товаров и показателей, их характеризующих, для выявления наиболее достоверных критериев идентификации;

- совершенствование стандартов, ТУ и другой нормативной документации путем включения в нее показателей качества для целей идентификации;

- совершенствование методов идентификации товаров, и в первую очередь экспресс-методов, позволяющих с достаточно высокой степенью достоверности определять все основополагающие характеристики товаров, особенно товароведные.

Объектами идентификации являются продукция, услуги, ценные бумаги (деньги, акции, векселя и др.), информация, рабочая сила и другие объекты коммерческой деятельности. В данном учебном пособии разберем лишь одну группу объектов – продукцию, которая вовлекается в процесс купли-продажи и становится товаром. Именно об идентификации продовольственных товаров в сфере торговли и у потребителя, приобретающего товары, пойдет речь, хотя следует отметить, многие рассматриваемые вопросы в равной степени могут быть отнесены и к непродовольственным товарам.

Субъектами, осуществляющими идентификацию товаров, являются все участники рыночных отношений: изготовитель – на стадии приемки сырья, полуфабрикатов, комплектующих изделий и при отпуске готовой продукции;

продавец – на стадиях заключения договоров купли-продажи, приемки товаров и подготовки их к продаже. Потребитель также проводит идентификацию приобретаемого товара, делая это чаще всего неосознанно и не имея достаточной квалификации, ориентируясь лишь на собственный житейский опыт и знания.

Классификации механизмов авторизации, реализованных в системах защиты:

- классификация по функциональному назначению(контроль загрузки, контроль функционирования);

- классификация по принадлежности идентификаторов и паролей(пользователь, ответственное лицо);

- классификация по субъекту их задания(администратор, пользователь, ответственное лицо) ;

- классификация по способу ввода идентификатора и пароля(ввод с клавиатуры, ввод с внешнего устройства);

- классификация по способу хранения идентификатора и пароля (локально на защищаемом объекте, удаленно на сервере).

3.1.4 Методы идентификации и установления подлинности субъектов и различных объектов

Объект идентификации и установление подлинности.

Идентификация- это присвоение какому-либо объекту или субъекту уникального образа, имени или числа. Установление подлинности (аутентификация) заключается в проверке, является ли проверяемый объект (субъект) в самом деле тем за кого себя выдает.

Объектами идентификации могут быть:

- человек (оператор, пользователь, оператор);
- техническое средство (терминал, дисплей, компьютер и т.д.);
- документы (распечатки, листинги и т.п.);
- носители информации (магнитные диски, ленты и т.п.);
- информация (табло, информация на дисплее).

Идентификация может быть произведена как специальным персоналом, так и техническими средствами.

Идентификация и установление подлинности личности. В качестве признака подлинности личности внешние признаки (рост, вес, формы отдельных частей тела и т.п.) правда со временем параметры человека меняются, но с развитием техники растет и точность прогнозирования этих изменений (отпечатки пальцев, голос и т.д.). Кроме антропологических параметров более внимательно необходимо относится к конфиденциальности, так как записанная информация на носителях является ключом к информации, подлежащей защите. Для этого существует система аутентификации “ключ-замок”. Система “ключ-замок” имеет локальный применение. Одним из распространенным методом аутентификации является присвоение лицу или объекту уникального имени или числа - пароля и хранение его в компьютерной системе. При входе в компьютерную систему пользователь открывает доступ к разрешенной только ему информации. Алгоритм идентификации компьютерной системы представлен (Рисунок . 3). Наиболее высокий уровень входа в систему разделение кода на две части: одну запоминаемую пользователем и вводимую вручную, вторую с помощью магнитной или иной карточкой.

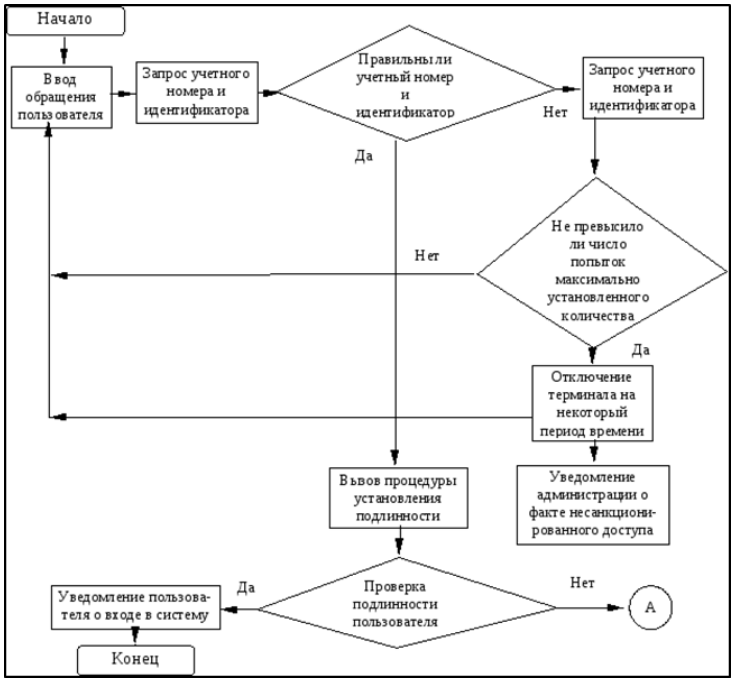

Рис. 3:

На случай защиты запоминаемой части пароля от получения ее нарушителем путем физического принуждения пользователя, возможно, будет полезно в вычислительной системе предусмотреть механизм тревожной сигнализации, основанной на применении ложного пароля. Ложный пароль запоминается пользователем одновременно с действительным и сообщается преступнику в экстренной ситуации.

Однако, учитывая опасность для жизни пользователя необходимо в компьютерной системе одновременно со скрытой сигнализацией предусмотреть механизм обязательного выполнения требований преступника, воспользовавшись средствами аутентификации законного пользователя.

Идентификация и установление подлинности технических средств. При организации системы защиты информационных процессов является идентификация подлинности технических средств. Данный уровень защиты осуществляется с помощью паролей. Пароль используется не только для пользователя и терминала по отношению к системе, но и для обратного установления подлинности компьютера по отношению к пользователю. Это используется для работы с удаленным объектом. В этом случае используются одноразовые пароли или более сложные системы шифрования информации.

Идентификация и установление подлинности документов. В компью-

терных системах документами являются распечатки, листинги, перфоленты, перфокарты, магнитные носители и т.д. Для этого случая используется два подхода: получение документа, сформированного непосредственно в КС и на ее документирования; получение ее с удаленных объектов КС. В первом случае подлинность гарантируется системой, имеющие средства защиты от НСД, а также физическими характеристиками печатающего устройства, присущие только этой системы. При недостаточности необходимо использовать криптографическое преобразование. Это особенно актуально для второго случая, когда документ доставляется через неохраняемую территорию с территории удаленного объекта. При этом к носителю прилагаются документы с подписями ответственных лиц, заверенными печатями. При неавтоматизированном обмене информацией подлинность документов удостоверяется личной подписью человека, автора документа. Проверка осуществляется визуально по личным документам. При автоматизированной передаче документов по каналам связи, расположенным на неконтролируемой территории, меняются условия обмена. Так как в этом случае подделка подписи документов является относительно простой, то используется так называемая электронная подпись. Этим пользуются организации занимающими банковскими и другими жизненно важной деятельностью. При этом участники нуждаются в защите от преднамеренных НСД в виде: отказа отправителя от переданного сообщения; изменения получателем полученного сообщения; маскировки отправителя под другого сообщения. Обеспечение защиты каждой стороны, участвующей в обмене информации, осуществляется с помощью ведения специальных протоколов. Для верификации используют следующие положения: отправитель вносит в передаваемую информацию свою электронную подпись, представляющую собой дополнительную информацию, зависящую от передаваемых данных, имени получателя и некоторой закрытой информации, который обладает только отправитель; получатель должен иметь возможность удостовериться в том, что в составе сообщения подпись есть подлинная подпись отправителя; получение правильной подписи отправителя возможно только при использовании закрытой информации, которой обладает только отправитель; для исключения возможности повторного использования устаревшего сообщения верификация должна зависеть от времени. Подпись сообщения представляет собой способ шифрования сообщения с помощью криптографического преобразования. Закрываемым элементом в преобразовании является код ключа. Идентификация и установление подлинности информации на средствах ее отображения и печати. В компьютерных системах с централизованной обработкой данных и относительно низкими требованиями к защите установлении ее подлинности на

технических средствах отображения информации гарантируется данной КС. Однако с усложнением системы увеличивается и вероятность возникновения НСД к информации, ее модификации и хищению. Поэтому в более ответственных случаях отдельные сообщения или блоки информации подвергаются специальной защите, которая заключается в создании средств повышения достоверности информации, ее криптографического преобразования. Установление подлинности полученной информации, включая отображение на табло и терминалах, заключается в контроле обеспечения достоверности информации, результатов дешифрования полученной информации до отображения ее на дисплее. Подлинность информации на средствах ее отображения тесно связана с подлинностью документов. Поэтому все положения приведены ранее справедливы и для этого случая. Чем ближе к полю отображения (бумажному носителю) эта процедура приближается, тем достовернее отображаемая информация.

3.1.5 Биометрическая аутентификация пользователей

Привычные системы аутентификации на сегодня не всегда удовлетворяют требованием политики информационной безопасности предприятия или компании. Все большую популярность набирает биометрическая аутентификация пользователя, разрешающая аутентифицировать пользователя с помощью считывания его физиологических данных. Методы аутентификация основывающийся на паролях имеют недостаток: многоразовый пароль можно скомпрометировать разными способами. USB-токкены и смарт-карты можно потерять, скопировать. Биометрические методы аутентификации не имеют эти недостатки. К основным плюсам таких методов относят: большой уровень достоверности аутентификации по биометрическим параметрам из-за их уникальности неотделимость биометрических параметров от пользователя; сложность фальсификации биометрических признаков. В качестве биопараметров используют следующие: форма кисти руки; отпечаток пальца; размер и форма лица; узор сетчатки глаза и радужной оболочки; особенности голоса. Схема работы биометрической системы аутентификации При процессе регистрации в системе пользователь должен показать один или несколько раз биометрический признак, по которому происходит дальнейшая аутентификация. Эти признаки в системе регистрируются как контрольный образец пользователя. Этот образец обрабатывается системой для получения ЭИП (эталонный идентификатор пользователя). ЭИП – числовая последовательность, из которой нельзя восстановить первоначальный образец. При прохождении аутентификации пользователем, сравнивается эталонные ЭИП и ЭИП при прохождении аутентификации. Поскольку

эти 2 параметра никогда не совпадут, существует параметр отвечающий за степень совпадения. На основе этой степени совпадения система решает о прохождении аутентификации. Ошибочный отказ (FRR)- это отказ, когда система не подтверждает законного пользователя. Такие отказы бывают 1 на 100. Ошибочное подтверждение (FAR) — подтверждение, когда система подтверждает аутентификацию незаконного пользователя. ТАкие ошибки бывают 1 на 10000. Дактилоскопическая система аутентификации Одна из причин широкого использования таких систем, это наличие громадных банков данных по отпечаткам пальцев. Основные пользователи таких систем являются сотрудники гос. служб или банковские компании. Основные компоненты дактилоскопической системы аутентификации: сканер ПО идентификации ПО аутентификации