Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Оренбургский государственный университет»

Р.Р. Галимов, А.А. Рычкова

**ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ**

Учебное пособие

Рекомендовано ученым советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по программам высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург

2017

УДК 004.3(076)

ББК 32.973.26-04я7

Г 15

Рецензент – кандидат технических наук, доцент Ю.И. Синицын

**Галимов Р.Р.**

**Г 15** Программно-аппаратные средства защиты информации в вычислительных системах: учебное пособие/ Р.Р. Галимов, А.А. Рычкова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 132 с.

Учебное пособие посвящено вопросам изучения принципов работы и практического применения программно-аппаратных средств защиты информации, представленных на российском рынке.

Учебное пособие предназначено для студентов вузов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность при изучении дисциплины «Программно-аппаратные средства защиты информации».

Пособие будет полезно преподавателям, слушателям потоков повышения квалификации по направлению информационной безопасности, а также специалистам-практикам в области защиты компьютерной информации.

УДК 004.3(076)

ББК 32.973.26-04я7

© Галимов Р.Р., Рычкова А.А., 2017

© ОГУ, 2017

# Содержание

|  |  |
| --- | --- |
| Введение……………………………………………………………………………… | 4 |
| 1 Задача защиты информации в вычислительных системах ……………………. | 5 |
| 1.1 Основные задачи защиты информации в компьютерных системах………… | 5 |
| 1.2 Основные нормативно-правовые документы, регламентирующие вопросы применения средств защиты информации………………………………………... | 6 |
| 1.3 Классификация вычислительных систем………………………………………. | 9 |
| 1.4 Классификация средств защиты информации в компьютерных системах…... | 14 |
| 2 Защита информации компьютерных систем от несанкционированного доступа…………………………………………………………………………………. | 19 |
| 2.1 Общая структура системы разграничения доступа…………………………… | 19 |
| 2.2 Подсистема аутентификации…………………………………………………… | 21 |
| 2.3 Виды аутентификации………………………………………………………….. | 24 |
| 2.4 Особенности систем разграничения доступа в операционных семействах Windows и Linux……………………………………………………………………... | 31 |
| 2.5 Программно-аппаратные средства защиты от НСД………………………….. | 37 |
| 2.5.1 Механизм доверенной загрузки……………………………………………… | 39 |
| 2.5.2 Аппаратные средства аутентификации и хранения ключевой информации. | 46 |
| 2.5.3 Замкнутая программная среда………………………………………………… | 49 |
| 2.5.4 Подсистема регистрации и учета…………………………………………….. | 52 |
| 3 Аппаратные средства хранения ключевой информации………………………. | 55 |
| 3.1 Идентификаторы iButton………………………………………………………. | 55 |
| 3.2 Система электронных платежей на основе iButton DS1963S……………….. | 57 |
| 3.3 Смарт-карты…………………………………………………………………….. | 62 |
| 3.4 USB-токены……………………………………………………………………… | 66 |
| 3.5 USB-токены с биометрической идентификацией…………………………… | 70 |
| 3.6 Электронные ключи с поддержкой открытого протокола двухфакторной аутентификации U2F………………………………………………………………….. | 71 |
| 3.7Устройства класса TrustScreen………………………………………………….. | 75 |
| 4 Электронная подпись и инфраструктура открытых ключей………………….. | 79 |
| 4.1 Электронная подпись……………………………………………………………. | 81 |
| 4.2 Цифровой сертификат стандарта X.509………………………………………. | 83 |
| 4.3. Усовершенствованная электронная подпись………………………………… | 87 |
| 4.4 Инфраструктура открытых ключей……………………………………………. | 89 |
| 4.5 Лабораторная работа. Инфраструктура открытых ключей Windows Server 2008…………………………………………………………………………………… | 93 |
| 5 Тесты для проверки знаний………………………………………………………. | 114 |
| Список использованных источников………………………………………………. | 126 |

**Введение**

Учебное пособие посвящено вопросам изучения принципов работы и практического применения программно-аппаратных средств защиты информации, представленных на российском рынке. Пособие состоит из четырех глав.

В первой главе описываются основные задачи обеспечения информационной безопасности (ИБ) в вычислительных системах, основные факторы, влияющие на выбор методов и средств защиты информации. Вторая глава посвящена принципам работы средств защиты от несанкционированного доступа (НСД) таких, как Dallas Lock, Secret Net, ПАК Соболь.

Третий раздел работы содержит теоретические сведения об аппаратных носителях ключевой информации, их архитектуре и возможностях. Рассмотрены вопросы применения аппаратных ключей в системах дистанционного банковского обслуживания. Вопросы использования электронной подписи и инфраструктуры открытых ключей рассмотрены в четвертой главе.

Учебное пособие предназначено для студентов вузов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность при изучении дисциплины «Программно-аппаратные средства обеспечения информационной безопасности».

Пособие будет полезно преподавателям, слушателям потоков повышения квалификации по направлению информационной безопасности, а также специалистам-практикам в области защиты компьютерной информации.

**1 Задача защиты информации в вычислительных системах и сетях**

* 1. **Основные задачи защиты информации в вычислительных системах**

С каждым годом увеличивается ценность информации для общества и государства, декларируются цели переходу к информационному обществу, безбумажной эре. При этом практически все информационные процессы реализуются на базе вычислительных систем и сетей. Большой объем ценной информации, обрабатывающейся в вычислительных системах, и доступность информационных технологий обуславливает важность задач обеспечения информационной безопасности.

В данной работе под вычислительной системой понимается совокупность взаимосвязанных и взаимодействующих процессоров или вычислительных машин, периферийного оборудования и программного обеспечения, предназначенная для подготовки и решения задач пользователей. Таким образом, в рассмотрение данной работы попадают такие вопросы, как защита информации на уровне аппаратного и программного обеспечения компьютера и вычислительной сети. При этом рассматриваются различные классы программных и программно-аппаратных современных средств защиты.

Защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию[1]. Цель защиты информации – предотвращение ущерба собственнику, владельцу, пользователю информации.

Основными задачами обеспечения информационной безопасности являются:

- защита информации от утечки;

- защита информации от несанкционированного воздействия;

- защита информации от непреднамеренного или преднамеренного воздействия;

- защита информации от разглашения;

- защита информации от несанкционированного доступа.

Выделяют два основных подхода для обеспечения информационной безопасности: фрагментарный и комплексный. Первый подход направлен на защиту от конкретных угроз, характеризуется высокой избирательностью. Основной недостаток фрагментарного подхода заключается в том, что изменение структуры автоматизированной системы или актуальных угроз приводит к снижению эффективности системы защиты информации[2].

Для больших и средних организаций предпочтительно использование комплексной системы обеспечения ИБ, объединяющий разнородные методы и средства защиты. Комплексный подход предполагает внедрение системы управления информационной безопасностью, включающий следующие основные процессы:

- анализ возможных угроз АС;

- планирование системы защиты;

- внедрение системы защиты;

- сопровождение системы защиты.

На этапе планирования системы защиты предприятия выбираются методы и средства, позволяющие снизить информационные риски. При этом необходимо учитывать множество факторов, такие как стоимостные и функциональные требования, соответствие требованиям нормативно-правовых документов. Целью данной работы является представление теоретических знаний о принципах работы основных программно-аппаратных средствах защиты информации.

* 1. **Основные нормативно-правовые документы, регламентирующие вопросы применения средств защиты информации**

Организационно-правовое обеспечения является важнейшей базой для построения системы защиты вычислительных систем и представляет собой её каркас, на который нанизываются остальные подсистемы, такие как инженерно-техническое обеспечение, криптографическое и программно-аппаратное обеспечение. Современной тенденцией в проектировании систем защиты информационных систем является необходимость применения комплексного подхода и модели многоуровневой защиты. Основой успешной реализации данной модели является эффективная политика информационной безопасности, обеспечивающая непротиворечивость и взаимосвязанность всех элементов системы защиты информационной системы.

Политика безопасности предприятия должна базироваться на нормативно-правовых документах, в которых зафиксирован мировой опыт в области защиты информации. На рисунке 1.2.1 представлена классификация нормативно-правовых документов.



Рисунок 1.2.1 –Классификация нормативно-правовых документов, регламентирующие вопросы обеспечения безопасности информационных систем

Основные цели организационно-правового обеспечения:

- обеспечение безопасной инфраструктуры для взаимодействия организаций;

- обеспечить информационную безопасность конкретного предприятия.

Требования и рекомендации международных организаций и государственных органов обеспечивают необходимый уровень защищенности и доверия между участниками информационных процессов. Международные документы имеют глобальное значение и представляют собой в большинстве случаев стандарты, позволяющие потребителям и разработчикам информационных систем оперировать общими терминами, понятиями и оценками. Примерами таких документов являются «ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», «ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Государственные организации издают документы, определяющие вопросы регулирования использования информационных систем и распространения информации с целью недопущения противоправных действий, ущерба другим участникам информационного обмена, обществу и государственным органам. Именно документы данного уровня являются обязательными.

Глобальные ИТ-компании разрабатывают методологическое обеспечение для эффективного использования своих популярных продуктов, в том числе с учетом вопросов информационной безопасности. В частности документ компании Microsoft по вопросам безопасности облачной технологии Windows Azure: «Рекомендации по обеспечению безопасности при разработке приложений Windows Azure»[3].

Но в большинстве случаев подобные документы ориентированы на типовые компьютерные информационные системы и в полной мере не учитывают особенности конкретного предприятия. В связи с этим в каждом предприятии разрабатывается политики безопасности, регламентирующие вопросы безопасности с учетом конкретных параметров КИС.

В данной работе рассматриваются документы, регламентирующие и рекомендующие использование определенных классов программно-аппаратных средств защиты вычислительных систем. Особую значимость приобретают документы, имеющие обязательный характер, не выполнение требований которых приводит к различным видам санкций, начиная от штрафов вплоть до приостановления или прекращения деятельности организации. В частности, при нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) предусмотрены штрафы[4].

Таким образом, выбор программно-аппаратных средств во многом определяется политикой безопасности предприятия, государственными нормативно-правовыми документами и международными стандартами.

* 1. **Классификация вычислительных систем**

Выбор программно-аппаратных средств защиты в большей степени зависит от параметров автоматизированной информационной системы. Для выявления характерных особенностей АИС, определяющих необходимость применения методов и средств обеспечения информационной безопасности, нужно рассмотреть их классификацию, представленную на рисунке 1.2.

Под монопольным режимом работы понимается использование информационной системы только одним сотрудником. Данный режим используется в малых организациях. Простым примером является случай, когда обработка данных осуществляется на одном компьютере одним пользователем. Преимуществом подобной схемы является использование более простых методов защиты информации, в частности от НСД. В многопользовательских системах задача обеспечения информационной безопасности усложняется в связи с тем, что необходимо правильно определить права доступа к общим ресурсам АС. При этом с увеличением количества пользователей возрастает вероятность, что среди них есть внутренний нарушитель. Данные обстоятельства определяют необходимость применения дополнительных мер защиты в отличие от однопользовательских систем, таких как очистка временных файлов и оперативной памяти[5].

Наиболее жестко регламентируются практически все вопросы обеспечения информационной безопасности для государственных информационных систем (ГИС), так как они обеспечивают функции государства. Примером нормативного документа, определяющего параметры системы защиты ГИС, является приказ ФСТЭК от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», где определены требования к мерам защиты. ГИС должны проходить процесс аттестации, определяющей соответствие мер защиты классу автоматизированной системы.



Рисунок 1.2 – Классификация информационных систем

Защита информационных систем коммерческих организаций является задачей собственника информационных ресурсов и во многом определяется необходимостью обеспечения экономической эффективности предприятия. Основными законами, регулирующими вопросы защиты информации, являются федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне",Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных", Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации". В зависимости от области экономической деятельности организации и типа обрабатываемых данных к ней могут предъявляться дополнительные требования государственных ведомств. В частности, для банковских системы выпущен отраслевой стандарт СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы российской федерации», определяющие основные требования по обеспечению ИБ. Несмотря на рекомендательный характер документа, большинство банков переходят на данный стандарт, так как он обеспечивает высокий уровень защищенности и перекрывает требования регуляторов по вопросам защиты персональных данных.

При использовании многопользовательской автоматизированной системы с разными полномочиями пользователей необходимо реализовать разграничение доступа ко всем ресурсам. В большинстве операционных системах, таких как Windows, Linux реализована ролевая модель доступа, являющейся модификацией дискреционной модели. Данная модель разграничения характеризуется высокими затратами на распределение полномочий к ресурсам системы. Основным недостатком подобной системы разграничения доступа является возможность владельца ресурса изменять права доступа, что может привести к утечке конфиденциальной информации. В связи с этим, для автоматизированных систем, обрабатывающих информацию, представляющих высокую ценность рекомендуется использование мандатный принцип контроля доступа. Например, в руководяще документе ФСТЭК [5] для СВТ класса защищенности 4 и выше определена необходимость использования мандатной модели доступа. Для соответствия данному требованию используются два типа решения:

- приобретение сертифицированной ОС с поддержкой мандатной модели доступа, например, ОС Astra Linux[6], МСВС[7]. Основой данных ОС является ядро Linux;

- установка специальных сертифицированных средств на операционные системы общего назначения, позволяющие реализовать мандатную модель доступа. Примерами таких СЗИ являются Dallas Lock, Secret Net.

Первый тип решения обеспечивает более высокий уровень защищенности, часто применяется в военных организация и при обработке информации, представляющей государственную тайну. Недостатками применения таких ОС является более высокая стоимость и ограничения использования прикладных программ, заключающейся в необходимости использования версий под ОС семейства Linux.

Второй способ позволяет минимизировать изменения в программных средствах автоматизированной системы. Позволяет организациям привести в соответствие с требованиями законодательства за короткий период.

Распределенная структура организации, наличие доступа в общедоступные сети, возможность удаленной работы сотрудников с подключением к корпоративной сети увеличивает число угроз информационной безопасности, что определяет необходимость применения определенных средств защиты, таких как межсетевые экраны, виртуальные частные сети.

Затраты на организацию защиты автоматизированной системы должны соотноситься с ценностью обрабатываемой информации. Для принятия решения об использовании мер по обеспечению информационной безопасности компьютерной системы используют понятие информационного риска, зависящего от вероятности реализации угрозы и уровня возможного ущерба. Ущерб организации определяется во многом ценностью информации и её количеством. Примерами влияния объема обрабатываемых данных на возможный ущерб организации являются утечки паролей почтовых служб, кражи данных о кредитных картах электронных магазинов, утечки персональных данных[8]. Все это определяет необходимость усиления мер защиты и использования более надежных средств защиты. В частности, в Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. приведена методика определения уровней защищенности ИПДН, зависящие от количества субъектов, ПДн которых обрабатываются в автоматизированной системе.

Выбор средств защиты зависит от типа используемых СВТ. Широкое применение мобильных устройств определяет актуальность вопросов их защиты от распространенных угроз информационной безопасности:

* нарушение конфиденциальности информации в результате кражи или утери устройства;
* нарушение конфиденциальности информации в результате доступа посторонних лиц к устройству, оставленному без присмотра;
* доступ к конфиденциальной информации внешних нарушителей посредством использования вредоносного программного кода;
* хищение информации работником, имеющим легитимный доступ к информации и хранящий эту информацию на своем устройстве (путем отправки через личную почту, выкладывания в dropbox и проч.)[9].

Использование мобильных устройств «разрывает» периметр безопасности автоматизированной системы предприятия, что требует применения в каждом устройстве целого комплекса СЗИ, таких как сетевой межсетевого экран, VPN-клиент, средства шифрования. Большинство операционных систем мобильных устройств имеют стандартные встроенные средства защиты[10], которые обеспечивают достаточно высокий уровень защищенности для работы с обычными данными. При обработке с персональными данными Российское законодательство требует использование средств шифрования, сертифицированных ФСБ и ФСТЭК. Данному требованию не соответствуют встроенные средства защиты и при этом в ряде ОС существует ограничения использования внешнего ПО, в частности в AndroidOS. В связи с этим разработчики СЗИ используют два пути:

- взлом мобильных устройств, с целью повышения уровня полномочий программного средства защиты;

- разработка своей доработанной версии ОС. Примером данного решения является планшет «Континент Т-10» фирмы «Код безопасности»[ 11, 12].

Популярность виртуальных сред увеличивает интерес злоумышленников к подобным системам. Механизмы защиты виртуальных сред во многом отличается от методов защиты физических серверов. В частности, трафик в виртуальной среде не может быть отфильтрован стандартным сетевым оборудованием, так как сетевой поток не покидает физический сервер. Также одновременный запуск антивирусных программ приведет к значительной нагрузке на физическое оборудование[13]. Еще одной проблемой является то, что виртуальные среды в большинстве случаев не поддерживают нестандартное аппаратное обеспечение. Под данный класс устройств попадают аппаратные средства защиты[14]. В связи с этим, для защиты виртуальных систем необходимы специальные средства защиты, такие как продукты компаний Catbird, HyTrust, «Код безопасности».

Таким образом, выбор программно-аппаратных средств защиты информации зависят от характерных особенностей автоматизированных систем.

* 1. **Классификация средств защиты информации в компьютерных системах**

Согласно ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" различают 4 основных вида защиты:

- правовая защита информации;

- техническая защита информации; ТЗИ:

- криптографическая защита информации:

- физическая защита информации.

При этом в литературе часто используется понятия программных и программно-аппаратных методов и средств защиты информации в компьютерных системах. В частности, в работе [15] вводится следующее определение: «К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав КС и выполняющие некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС».

Большое количество разнообразных угроз компьютерных систем определяет необходимость применения разнообразных средств защиты. При этом необходимо обеспечить приемлемые оценки рисков информационной безопасности при минимальных затратах на построение и эксплуатацию системы защиты КС. Эффективность системы защиты компьютерной системы во многом определяются средствами защиты, выбор параметров зависит от множества факторов, в том числе и характеристик СЗИ.

Для определения характеристик средств защиты информации разработана их классификация, представленная на рисунке 1.3.



Рисунок 1.3 – Классификация средств защиты

В связи с необходимости обеспечения комплексного подхода к построению систем защиты увеличивается степень интеграции различных функций в одном СЗИ, которые по назначению могут принадлежать сразу нескольким классам. Одной из важнейших задач для обеспечения ИБ является контроль эффективности применения систем защиты, зависящей не только от наличия СЗИ, но их от оптимальности их настроек. Для выявления фактического уровня защищенности компьютерной системы используются такие СЗИ, как «Сканер-ВС», «XSpider», «Nessus Scanner», «MBSA». Данные средства позволяют автоматизировать поиск уязвимостей компьютерной системы за счет тестирования и сбора информации о её конфигурации и тестирования системы защиты на взлом. При этом необходимо отметить наличие сертификатов ФСТЭК у «XSpider» и «Сканер-ВС».

Криптографические средства защиты позволяют обеспечить конфиденциальность информации, являются эффективным инструментом защиты от НСД в многопользовательских информационных системах. Особенно актуальной применение механизма шифрования при использовании общедоступных сетей передачи данных, например, при удаленной работе с ресурсами компьютерной системы через VPN. Незаменимо применение средств шифрования в системах электронной отчетности, дистанционного банковского обслуживания для подтверждения подлинности электронных документов и обеспечения их актуальности.

Важнейшей задачей обеспечения информационной безопасности КС является защита от НСД. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа. К таким мерам относятся использование межсетевых экранов, средств криптографического преобразования данных. Особое место занимают СЗИ от НСД, используемых для защиты рабочих станций и серверов, реализующие такие функции, как двухфакторная аутентификация, доверенная загрузка ОС, контроль целостности программного и аппаратного обеспечения, блокирования ПК при обнаружении попыток несанкционированного доступа, регистрация действий субъектов и запущенных процессов. Примерами подобных сертифицированных средств защиты являются продукты «Dallas Lock», «Secret Net», «Страж NT», ПАК «Соболь», «Аккорд-АМЗД» и другие.

В связи с наличием у большинства компьютерных систем доступа к общедоступным сетям, в частности, к сети Интернет все более актуальными становятся сетевые угрозы. Применение межсетевых экранов является сегодня необходимостью, позволяя блокировать нежелательный сетевой трафик. Также использование сертифицированных МСЭ позволяет разграничить сегменты информационной системы, требующие обеспечения более высокого уровня ИБ, с целью снижения затрат на построение системы защиты информации.

Межсетевые экраны являются одной из первых линий эшелонированной системы защиты, но при этом не могут обеспечить полную сетевую ИБ вследствие следующих причин: недостатки проектирования и применения[16]. В связи с этим существует необходимость систем обнаружения и предотвращения вторжений, автоматизирующих процесс анализа больших объемов данных аудита. Развитие каналов связи увеличивает мобильность сотрудников, но при этом возрастают угрозы связанные с удаленным доступом к корпоративной сети с использованием общедоступных каналов связи. Основным методом защиты является шифрование сетевого трафика на основе виртуальных частных сетей.

С развитием технологий увеличивается риск утечки конфиденциальных документы в результате действий собственных сотрудников компании. Использование средств шифрования данных, систем разграничения доступа не позволяет полностью перекрыть все возможные каналы передачи данных, что определяет необходимость применения DLP-систем.

Многие параметры средств защиты, такие как стоимость, устойчивость к модификации, гибкость, зависят от способа реализации. Программные средства защиты характеризуются многообразием функций, простотой тиражирования, более низкой стоимостью по сравнению с аппаратными решениями. К недостаткам СЗИ данного класса относится:

- потребление вычислительных ресурсов ПК, для реализации функций защиты;

- низкая производительность в связи с тем, что программы исполняются универсальными процессорами, а не специализированными. При этом на ПК могут выполняться параллельно другие процессы;

- пристыкованность многих программных СЗИ к КС, что создает для злоумышленника потенциальную возможность обхода;

- возможность модификации злоумышленником программных средств защиты;

- имеются ограничения по использованию на определенных типах операционных систем;

-качество реализации функций защиты информации на программном уровне может уступать аппаратным, например, генерации случайных чисел для криптографических преобразований.

В связи с тем, что программные средства могут быть изучены или модифицированы злоумышленником, то применение подобных СЗИ ограничен для компьютерных систем требующих высокий уровень ИБ.

Большинства недостатков программных СЗИ лишены аппаратные решения, которые имеют такие отличительные особенности как аппаратный генератор случайных чисел, парафазные шины, препятствующие утечки информации по каналам ПЭМИН, загрузка ключей шифрования производится непосредственно в аппаратное устройство, минуя ОЗУ и системную шину ПК. Применение специализированных вычислительных средств усложняет задачу изучения принципов работы СЗИ.

Основным недостатками аппаратных средств защиты являются небольшой набор функций и наличие ограничений с учетом небольшого объема ресурсов, в частности, данные СЗИ характеризуются небольшим объемом памяти для хранения журналов событий. Также имеются ограничения возможности использования устройств данного класса, определяющиеся отсутствием на СВТ соответствующих интерфейсов.

**2. Защита информации от несанкционированного доступа**

**2.1 Общая структура системы разграничения доступа**

Задача защиты информационных ресурсов от несанкционированного доступа является одной из основополагающих в области ИБ. НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС[17].

Основными способами защиты информации от НСД в АС является корректная и надежная реализация системы разграничения доступа (СРД) субъектов к объектам. Общая схема СРД представлена на рисунке 2.1



Рисунок 2.1 –Структурная схема системы разграничения доступа

Диспетчер доступа, получив запрос на выполнение определенных операций над ресурсом, проверяет уровень полномочий субъекта с учетом ПРД и принимает решение: разрешить или блокировать. Сбой в работе системы разграничения доступа или вспомогательных подсистем, некорректные правила разграничения доступа позволяют нарушителю получить несанкционированный доступ к информации. Для обеспечения возможности проведения расследований инцидентов ИБ факт доступа и его параметры фиксируются в журнале событий.

Качество СРД определяется характеристиками обеспечивающих средств, выполняющих следующие функции:

- идентификацию и аутентификацию субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

- регистрацию действий субъекта и его процесса;

- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

- тестирование;

- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

- учет выходных печатных и графических форм и твердых копий в АС;

- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Современные операционные системы реализуют системы разграничения доступа на достаточно высоком уровне. Основным недостаткам СРД подобных систем является, что их сложно проверить на наличие недекларированных возможностей в связи с тем, что придется проверять всю сложную ОС. В связи с этим, на рынке представлены специализированные сертифицированные программно-аппаратные средства защиты от НСД, такие как ПАК «Соболь», Secret Net, Dallas Lock, Страж NT, которые дублируют функции операционной системы и позволяют привести АС в соответствие с законодательством. Причем подобные системы могут реализовать различные модели доступа.

Распространенными моделями разграничения доступа, получившие практическую реализацию, являются:

- дискреционная модель разграничения доступа;

- мандатная модель разграничения доступа;

- ролевая модель разграничения доступа.

Модели дискреционного доступа представляют КС как совокупность некоторых множеств взаимодействующих элементов, и множество допустимых доступов определяется набором объектов: пользователь - операция - объект[18]. Основным достоинством данной модели разграничения доступа является гибкость настройки прав доступа. Но для систем с большим количеством ресурсов и пользователей увеличивается нагрузка на администратора. Решением данного недостатка является использование ролевой модели, которая заключается объединении субъектов в группы, согласно выполняемым им ролям. При этом права доступа настраиваются не каждому пользователю, а группе. Еще одним недостатком данных моделей разграничения доступа является возможность владельца изменять настройки прав доступа для объектов, который сам создал. Это обстоятельство позволяет пользователю преднамеренно или непреднамеренно предоставить доступ злоумышленнику.

Избирательная (мандатная) модель доступа основана на использование меток конфиденциальности для объектов доступа и уровня разрешения для субъекта. Для определения доступа к объекту используются следующий алгоритм:

- при совпадении уровня доступа и метки конфиденциальности субъект может выполнить операции чтении и записи;

- если уровень доступа меньше значения метки конфиденциальности, то субъекту запрещен все операции;

- если уровень доступа больше значения метки конфиденциальности, то субъекту разрешается только чтение, запись запрещена.

Важным достоинством данной модели является то, что пользователь не может управлять доступом к создаваемым им ресурсам. Создаваемым объектам информационной системы присваивается в качестве метки конфиденциальности уровень доступа пользователя.

**2.2 Подсистема аутентификации**

Эффективность системы разграничения доступа зависит от качества реализации подсистемы аутентификации. С учетом определенных актуальных угроз ИБ и класса автоматизированной системы применяются различные методы аутентификации. Процесс регистрации в системе пользователя включает три основных взаимосвязанных процесса: идентификация, аутентификация и авторизация.

Идентификация – это процедура распознавания пользователя по его идентификатору, присвоенного и занесенного в базу данных его при регистрации[19]. При входе в компьютерную систему проверяется идентификатор пользователя на наличие в базе данных. Таким образом, скрытие идентификатора пользователя от чужих глаз усложняет возможность НСД для злоумышленника.

После идентификации выполняется процедура аутентификации, заключающейся в проверке подлинности субъекта компьютерной системы. При этом субъект предоставляет определенную секретную информацию, доступную только ему. Данную информацию в дальнейшем будем называть фактором аутентификации[20]. Субъекты системы выполняют аутентификацию тремя основными способами:

- на основании знания чего-либо (пароль, PIN-код);

- на основе обладания чего-нибудь (аппаратный ключ, магнитная карта, одноразовый пароль);

-на основе биометрических характеристик (отпечаток пальца, рисунок сетчатки глаза, голос)[21].

В качестве четвертого фактора аутентификации рассматривают информацию о месте проведения процедуры[20]. Примером может являться политика разрешения проведения аутентификации только с определенного компьютера, расположенного в помещении с ограниченным физическим доступом. Данный способ проверки подлинности может работать только совместно с другими видами. Дальнейшим развитием данного направления процедуры проверки подлинности является интеграции систем аутентификации с СКУД. Примером реализации подобного подхода является комплекс «Рассвет-СВМиКД» фирмы ОКБ САПР[22], позволяющей интегрировать систему контроля доступа, видеонаблюдения и защиты от НСД. Преимуществами данного решения являются:

- дополнительные проверки при выполнении процедур аутентификации (авторизации) пользователей повысят уровень информационной безопасности;

- уменьшение количества паролей, запоминаемых пользователем, и всевозможных персональных носителей-идентификаторов уменьшит число инцидентов безопасности, в том числе связанных с халатностью или другими персональными особенностями сотрудников;

- снижения числа событий, предотвращение и анализ которых требует преимущественно организационных мер и значительно зависит от человеческого фактора[23].

Также существует тенденция интеграции аппаратных ключей с радиочастотными метками RFID, позволяющие использовать их как для доступа к помещению, так и для аутентификации в компьютерной системе. Примерами подобных устройств являются Рутокен S RF, возможно варианты исполнения с радиочастотной меткой для аппаратных ключей eToken. Типичным сценарием использования подобных устройств является следующее: радиочастотная метка используется для доступа в защищенное помещение с компьютером, а секретная информация, скрытая в аппаратном ключе, используется для аутентификации в компьютерную систему.

Для того чтобы обеспечить управление и контроль над данными процедурами, дополнительно используются процессы администрирования и аудита.

Под администрированием понимается процесс управления доступом субъектов к ресурсам системы и включает в себя:

- создание идентификатора субъекта (создание учетной записи) в системе;

- управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата);

- управление правами доступа субъекта к ресурсам системы.

Аудит - процесс контроля доступа субъектов к ресурсам системы, включающей протоколирование их действий в целях обеспечения возможности обнаружения несанкционированных действий[20].

В зависимости от требований к системам защиты информации могут быть использованы различные комбинации в применении процессов администрирования и аудита. В данном контексте выделяют 2 основных класса информационных систем в зависимости от применения вспомогательных процессов системы разграничения доступа:

- системы, реализующие процедуры аутентификации, авторизации и администрирования, 3A;

- системы, реализующие процедуры аутентификации, авторизации, администрирования и аудита, 4A.

Для обеспечения ИБ компьютерной системы важной задачей является выбор способа аутентификация.

**2.3 Виды аутентификации**

Важность процесса аутентификации во многом определило большое разнообразие методов аутентификации, различающиеся различными характеристиками, такими как уровень обеспечения информационной безопасности, сложности реализации и стоимостных затрат. Для выбора метода аутентификации для определенной компьютерной системы необходимо определить особенности данной процедуры. В связи с этим разработана классификация методов аутентификации, представленная на рисунке 2.2.

Выбор метода аутентификации определяется необходимостью обеспечения требуемого уровня ИБ, зависящей от ценности информационных ресурсов компьютерной системы. По данному признаку различают следующие классы методов аутентификации: простая, строгая и биометрическая[19]. Простая аутентификация основывается на использование паролей, основными характеристиками которой являются минимальные затраты на реализацию. Недостатками данного подхода является то, что обеспечивается низкий уровень информационной безопасности. Это определяется тем, что пользователю требуется запоминать или хранить пароль, что приводит к использованию паролей с плохой устойчивостью к атакам по их подбору. Также увеличивается вероятность разглашения пароля другим лицам. Такие ситуации возникают, когда сотрудник организации отсутствует на рабочем месте, а его коллегам срочно требуются определенные документы, доступ к которым возможен только под определенной учетной записью. Пароль при этом часто сообщается по телефону.

Строгая аутентификация предполагает использование нескольких факторов. Наиболее распространенной реализацией является двухфакторная аутентификация на основе аппаратных ключей, таких как Рутокен, eToken. Использование аппаратных носителей позволяет хранить более сложные пароли, цифровые сертификаты в их защищенной памяти в сравнении с простой аутентификацией. Основными факторами аутентификации в данном случае является признак обладания аппаратным ключом и PIN-код, позволяющий получить доступ к хранимой информации. Строгая аутентификация применяется в системах дистанционного банковского обслуживания, сдачи электронной отчетности, проведения аукционов. Недостатками данного класса является увеличение затрат на приобретение аппаратного носителя. При взаимодействии с государственными сервисами часто требуется приобретение цифрового сертификата.



Рисунок 2.2 –Классификация методов аутентификации

Наиболее дорогостоящим решением для рабочих станций является использование биометрической аутентификации, которая определяет необходимость приобретения специальных аппаратных средств - сканеров отпечатков пальцев. Также решения по данному классу аутентификации характеризуются вероятностью возникновения ошибок первого и второго рода. Это объясняется тем, что задача распознавания подобных данных плохо формализуются. Особенно высока оценка вероятности ошибки не допуска зарегистрированного пользователя при случайных воздействиях на биометрические характеристики, например, порезы на пальцах, изменение тембра голоса в результате простудных заболеваний. Достоинством биометрической аутентификации является сложность передачи аутентификаторов другому пользователю, обеспечивается эффект присутствия человека на месте аутентификации. Также сокращается время проведения процесса аутентификации, так как операция ввода данных автоматизирована и часто совмещена с процессом идентификации. Данный вид аутентификации привычно применялся в банковской сфере для ограничения доступа в помещения. В связи с развитием вычислительной мощности мобильных устройств и наличием средств регистрации биометрических характеристик находят применение в них аутентификация по отпечатку пальцев, по изображению лица, по рисунку сетчатки глаза, по голосу[24, 25]. Дополнительными недостатками данного метода являются то, что реализуется в определенной степени вмешательство в частную жизнь, вызывает отторжение у людей по религиозным, культурным, гигиеническим причинам, непригодность для пользователей, у которых отсутствую части тела.

Системы аутентификации на основе долговременных паролей характеризуются низкой стойкостью в связи с тем, что их можно подсмотреть, перехватить, разгадать или украсть. Более высокий уровень безопасности обеспечивают одноразовые пароли (One Time Password, OTP), генерируемые для единичного использования с помощью программных или аппаратных аутентификационных устройств. Одноразовый пароль используется в течение ограниченного интервала времени, что делает практически бесполезным сетевой перехват. Типовой схемой применения OTP-систем является следующее:

- OTP-токен пользователя генерирует случайное значение ***K*** по некоторому алгоритму с учетом предыдущего цикла аутентификации;

- пользователь отправляет в зашифрованном виде значение ***K*** серверу аутентификации;

- сервер проверяет полученное значение со своим сгенерированным.

Для работы данной схемы необходимо, чтобы OTP-токен и сервер генерировали одинаковые значения.

Простейшим примером одноразовой аутентификации является использование разделяемого списка секретных паролей, каждый из которых используется только один раз. Такая схема часто применяется в системах интернет-банк, в частности в банках Росбанк, Сбербанк[26, 27]. Для распределения данного списка используются банкоматы, специальные мобильные приложения. Разновидностью одноразового пароля являются также SMS-пароли.

Часто для генерации одноразового пароля используется аппаратный OTP-токен. Примерами таких устройств являются eToken PASS, токены-генераторы одноразовых паролей (OTP) ActivID. Они изготавливаются в различных форматах: OTP-калькулятор, брелок, смарт-карты. Дополнительным элементом защиты для данных устройств является использование PIN-кода. На стороне сервера обычно размещается программные комплексы, связанные с комплектами аппаратных OTP-токенов и генерирующие соответствующие одноразовые пароли. Преимуществом аппаратных токенов является в отсутствии необходимости подключения к рабочей станции, что становится актуальной с развитием мобильных вычислительных устройств, в которых часто нет стандартных интерфейсов.

Несмотря на достоинства данного метода аутентификации в сравнении с использованием статических паролей, что он не может обеспечить уровень защищенности сопоставимой с использованием сертификатов. В частности, в системах с удаленными пользователями при использовании одноразовых паролей используется в лучшем случае одностороннее SSL-соединение, что определяет возможность атаки «человек по середине»[ 28].

Таким образом, аутентификация на базе одноразовых паролей хоть и является более стойкой по сравнению многоразовыми паролям, но все равно для обеспечения требуемого уровня доверия определяет необходимость применения специальных мер:

- применение временных задержек для предотвращения возможности подбора пароля;

-временное блокирование при многократных ошибках ввода OTP-пароля;

- использование CAPTCHA;

- применение механизма «запрос-ответ»;

- использование аппаратных OTP-токенов с дополнительной защитой в виде PIN-кода.

Процесс аутентификации с использованием цифровых сертификатов (ЦС) считается одним из самых стойких при обеспечении мер надежного хранения закрытого ключа. Достоинствами использования ЦС являются:

-позволяют взаимно проверить подлинность участников аутентификации: как пользователя, так и сервера аутентификации;

- минимизируется проблема распространения ключевой информации между пользователями системы.

Типовой алгоритм аутентификации с использованием цифровых сертификатов представлен на рисунке 2.3. Вся схема аутентификации базируется на использование открытых протоколов шифрования, механизма рукопожатия и доверия к третьей стороне – доверенному центру сертификации (ЦС).

Перед началом процесса взаимной аутентификации участники должны получить от ЦС следующие элементы:

- сертификат участника процесса проверки подлинности с его открытым ключом и заверенным центром сертификации электронной подписью: ***CertA*** и ***CertB*** соответственно для объектов ***A*** и ***B***;

- соответствующие сертификатам ***CertA*** и ***CertB*** их закрытые ключи ***Ka*** и ***Kb***;

- доверенный сертификат ЦС ***CertC***.



Рисунок 2.3 – Общая схема аутентификации на основе цифровых сертификатов

После получения соответствующих сертификатов появляется возможность произвести процесс аутентификации:

- процесс проверки подлинности инициирует пользователь ***A***. При данном запросе на сервер могут передаваться данные о поддерживаемых протоколах аутентификации и алгоритмов шифрования;

- при успешном согласовании протоколов и алгоритмов сервер возвращает идентификатор данного процесса аутентификации ***tokenID*** и генерирует случайное число ***tokenBA***, который будет использоваться для проверки подлинности пользователя ***A***;

- пользователь ***A*** отправляет свой сертификат и зашифровывает своим закрытым ключом ***Ka*** случайное число ***tokenAB***, состоящий из 3 элементов: ***RanA***- случайное число сгенерированное клиентом ***A***, полученный от сервера ***tokenBA*** и ***nameB*** - имя сервера ***B***;

- если сервер успешно проверит сертификат клиента ***CertA*** с использование открытого ключа центра сертификации и в результате расшифровки ***tokenAB*** убедиться, что пользователь вернул правильное значение tokenBA и имя сервера nameB, то считается что пользователь ***A*** успешно прошел аутентификацию;

- в ответ сервер ***B*** отправляет пользователю сертификат CertB и зашифрованный ***tokenBA***, содержащий ***ranA***, ***ranB*** и имя клиента ***nameA***. Пользователь А, расшифровав сертификатом сервера ***tokenBA***, проверяет ранее сгенерированное случайное число ***ranA***, производя аутентификацию сервера. Проверка значения ***nameA***, позволяет пользователю удостоверится, что процесс аутентификации производится именно для него[29].

Таким образом, аутентификация при помощи цифровых сертификатов позволяет произвести взаимную аутентификацию по общедоступным сетям, при этом не требуется активного участия третьей стороны. Основным недостатком подобного способа аутентификация являются затраты на развертывания инфраструктуры открытых ключей.

Современные информационные системы содержат большое количество служб, приложений, большинство из которых в целях обеспечения безопасности требую выполнить процедуру аутентификации. Пользователь вынужден хранить большое количество идентификаторов и паролей, которые очень тяжело запомнить, что вынуждает их записывать на бумаге. Это увеличивает риск того, что аутентифирующий параметр узнает злоумышленник. Дополнительным негативным фактором является сложность администрирования учетных записей[19, 30].

Данные недостатки решают схемы с однократного входа с авторизацией SSO (Single Sign-On), позволяющие однократно пройти аутентификацию и получить доступ к авторизованным ресурсам. SSO-системы выполняют аутентификацию централизованно, но для авторизации имеются два основных варианта:

- авторизация на целевом объекте;

-централизованная авторизация.

Схемы однократного входа поддерживают протоколы LDAP, SSL, Kerberos, архитектура открытых ключей. Решения SSO характеризуются различной степенью сложностью и функциональности: начиная от простых, реализующих псевдо SSO, до средств уровня всего предприятия, таких как Global Sign-On IBM, Trust-Broker Security Suite от CyberSafe.

Таким образом, существует различные классы механизмов аутентификации, отличающиеся рядом параметров. Выбор конкретных решений определяется критериями обеспечения высокого уровня ИБ, функциональности АС и стоимостных затрат на реализацию.

**2.4 Особенности систем разграничения доступа в операционных семействах Windows и Linux**

2.4.1 Система разграничения доступа операционной системы Windows

Важнейшим элементом системы безопасности операционной системы Windows является система разграничения доступа, базирующаяся на дискреционной модели. При этом различают два основных способа аутентификации: локальную и доменную. Доменная аутентификация является предпочтительной для АС с большим количеством компьютеров. В данной работе рассматривается локальная аутентификация, так как позволяет достаточно просто представить особенности системы разграничения доступа данной операционной системы.

Компоненты системы разграничения Windows доступа имеют модульную структуру и основными её службами являются:

- процесс регистрации запросов пользователей WinLogon, который инициирует интерактивную процедуру аутентификации и отображает диалоговое окно для ввода логина и пароля как при локальном входе в систему, так и при удаленном;

- сервис локальной безопасности (Local Security Authority, LSA), который координирует работу всех остальных модулей. Он порождает маркеры доступа, управляет локальной политикой безопасности и предоставляет интерактивным пользователям аутентификационные услуги. LSA также контролирует политику аудита и ведет журнал, в котором сохраняются сообщения, порождаемые диспетчером доступа[31]. Данный сервис получает логин и пароль от WinLogon и передает их диспетчеру учетных записей безопасности (Security Account Manager,SAM);

- диспетчер учетных записей безопасности (Security Account Manager, SAM) управляет базой данных с информацией о пользователях и группах пользователей в системе;

- монитор состояния защиты (Security Reference Monitor, SRM) отвечает за проверку прав доступа к объектам, манипулирование привилегиями (правами пользователей) и генерацию сообщений аудита безопасности.

На рисунке 2.4 представлена общая схема основной части системы безопасности операционных систем Windows – системы аутентификации.



Рисунок 2.4 – Структурная схема локальной системы аутентификации ОС Windows

Введенный логин и пароль пользователя от службы Winlogon передается сервису локальной безопасности, который рассчитывает хеш-функцию над паролем ***HA***. Также служба LSA запрашивает по идентификатору ***Id*** пользователя у диспетчера учетных записей хеш ***Hb***, сохраненный при регистрации. Аутентификация пользователя производится сравнением значений ***Ha*** и ***Hb***. Политика безопасности LSA определяет настройки службы, например, количество неправильных попыток для вход в систему. Результаты аутентификации фиксируются в журнале событий и передаются монитору состояния защиты, контролирующему запросы к ресурсам системы в соответствии с правами доступа.

После аутентификации в системе пользователь получает маркер доступа (token), который содержит:

- идентификаторы пользователя (SID);

- идентификаторы групп, в которые входит пользователь;

- список прав доступа по умолчанию DACL;

- системные привилегии[32 ].

Список DACL используется для присвоения создаваемым процессами пользователя объектам прав доступа по умолчанию. Параметр системные привилегии определяет разрешенные операции с системными объектами операционной системы. Например, системные привилегии маркера доступа задают возможность пользователю управлять аудитом и журналом безопасности, завершать работу системы, стать владельцем объектов безопасности системы[33]. Каждый запускаемый процесс пользователя получает данный маркер доступа.

Доступ к объектам безопасности операционной системы Windows задается дескриптором безопасности (Security Descriptor, SD), состоящий из следующих основных элементов:

- идентификатор владельца объекта (SID);

- пользовательский список управления доступом (Discretionary Access Control List, DACL), который формируется владельцем и определяет права доступа для других пользователей;

- системный список управления доступом, (System Access Control List, SACL), определяющий перечень действий над объектом, подлежащих аудиту[34].

Каждый элемент ACE (Access Control Entries, ACE) списка доступа DACL состоит из следующих полей:

- идентификатор пользователя или группы для которых определено права доступа к объекту;

- непосредственно права доступа;

- тип записи, определяющее разрешение или запрет прав доступа;

- флаги, определяющие механизмы наследования прав доступа для вложенных объектов, например, для файлов папок.

Запросы процессов, запущенных от имени определенной учетной записи, обрабатываются монитором состояния защиты, принимающего решение на основании маркера доступа и дескриптора защиты объекта доступа. Запрос характеризуется запрашиваемыми типами операций над объектом: чтения (***R***), записи (***W***) или выполнения (***E***).

Доступ к объекту разрешается, если разрешение всем операциям из запроса встречается с начала списка управления доступа DACL раньше, чем запрет хотя бы для одной операции. Причем рассматриваются элементы ACE, соответствующие пользователю или группе вхождения. Запрещающие правила имеют более высокий приоритет и размещаются ОС в начале списка доступа[33,34]. На рисунке 2.5 запрос от процесса А заблокирован, так присутствует запрет в ACE1 для данного пользователя. Доступ второго процесса разрешен, так как в списке DACL отсутствует запрет для чтения для второго пользователя и его групп.



Рисунок 2.5 – Схема организации запроса доступа к объекту

Особое значение имеет владелец объекта, который может изменить список прав доступа DACL, даже если у него запрещен любой тип доступа. Администратор может стать владельцем любого объекта и соответственно определить их права доступа. Механизмы наследования, ролевая дискреционная модель доступа позволяют гибко настроить права доступа пользователей. Основной недостаток – это возможность предоставить доступ владельцем объекта другим, что является характеристикой дискреционной модели доступа. Второй момент – степень довериям к реализации функциями аутентификации и наличие уязвимостей ОС, которые определяются сложностью системы Windows.

2.4.2 Система разграничения доступа операционных семейства Linux

Операционная система Linux базируется на принципах Unix, в том числе и в вопросах механизмов обеспечения информационной безопасности. Основными объектами доступа являются объекты файловой системы. Все субъекты доступа делятся на три основных класса:

- владельцы объектов файловой системы;

-члены групп, к которым принадлежит владелец объекта файловой системы;

- остальные пользователи системы.

Основными операциями над объектами доступа являются: чтение (***R***), запись(***W***) и выполнение (***E***). Права доступа к объекту определяются списком, состоящим из 9 признаков (три тройки) и определяющие возможности выполнения операции для трех типов пользователей[32]. На рисунке 2.6 представлена общая схема доступа к объекту.



Рисунок 2.6 - Схема организации доступа в ОС семейства Linux

Проверка прав доступа осуществляется в следующем порядке:

- проверка идентификатора владельца;

- проверка идентификатора группы.

При совпадении идентификатора доступ определяется соответствующей группой прав. Иначе используются разрешения для всех других пользователей.

В целом, современные операционные системы семейства Linux и Windows предоставляют механизм для повышения уровня безопасности за счет правильной настройки прав доступа к объектам. Основными недостатками СРД операционных систем являются невысокое качество реализации и наличие уязвимостей у вспомогательных подсистем, таких как систем аутентификации, контроля целостности аппаратно-программных средств, обеспечения безопасной загрузки ОС. Современные ОС ориентированы в большей степени на обеспечение высокой производительности за счет снижения качества средств обеспечения ИБ. Также возможны ошибки в программном коде операционной системы, которые приводят к появлению новых уязвимостей информационной безопасности. В связи с этим, существует необходимость в АС, обрабатывающих конфиденциальную информацию, применение либо специализированных ОС, характеризующихся высокой степенью защищенности, либо установка аппаратно-программных средств защиты от НСД.

**2.5 Программно-аппаратные средства защиты от НСД**

В организациях, обрабатывающих конфиденциальную и секретную информацию, требуется гарантировать высокую степень доверия к элементам компьютерной системы. Для того чтобы компьютерной системе можно было полностью доверять, её необходимо аттестовать:

- определить множество выполняемых функций;

- доказать конечность этого множества;

- определить свойства этих функций[2].

Сложность современных ОС, заключающееся в большом размере их кода, не позволяет полностью определить множество выполняемых функций системы. Также это приводит к наличию уязвимостей связанных с наличием ошибок в программном коде. Данное обстоятельство усложняет возможность обнаружения не декларированных возможностей и программных закладок, особенно для ОС с закрытым исходным кодом. В связи с этим, современные компьютерные системы в большинстве своем относятся к классу частично контролируемых, для которых не существует полных гарантий отсутствия ошибок, уязвимостей и аппаратно-программных закладок.

В случае, когда информационные риски автоматизированной системы не приемлемы, возможны следующие меры обеспечения требуемого уровня информационной безопасности:

- изоляцией от злоумышленника ненадежной компьютерной среды, её компонентов, процессов с помощью полностью контролируемых средств;

- использованием полностью контролируемых программно-аппаратных средств, выполняющих определенные защищенные операции для наиболее критичных с точки зрения ИБ функций и играющих роль специализированных модулей безопасности;

- применение полностью контролируемых средств ВТ.

Примером применения первой схемы является обработка конфиденциальной информации на компьютерах в специально выделенных помещения без доступа в вычислительные сети. Информационная безопасность обеспечивается в основном организационными и физическими методами защиты информации. Несмотря на эффективность подобного решения, основным недостатком является снижение функциональности системы, в частности, из-за ограничения возможности обмена информацией по вычислительным сетям.

Разработка полностью контролируемых операционных систем представляет собой трудоемкий процесс. Разработанные отечественные ОС, такие как Astra, являются модификацией Linux- систем. При этом есть ограничения по возможности установки типовых программных комплексов и средств, в большинстве своем разработанных за рубежом, особенно ориентированных на ОС Windows. Возникают дополнительные затраты на обучение персонала. Данные ограничения определяют оптимальность применения подобных решений для защиты информации в специализированных организациях, где возможные значения ущерба в результате инцидентов с ИБ превышают дополнительные затраты.

Для коммерческих организаций в большинстве случае подходит установка специализированных полностью контролируемых СЗИ на стандартные средства вычислительной техники. Немаловажным достоинством применения подобного подхода, кроме повышения уровня защищенности АС, является возможность обеспечить соответствие параметров ИС требованиям регулятора в области ИБ, в частности требованиям использования сертифицированных СЗИ определенного класса.

2.5.1 Механизм доверенной загрузки

Средство доверенной загрузки – программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы[35]. Данный класс СЗИ дополняет возможности стандартных ОС и предназначены для защиты от следующих видов угроз:

- блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

- контроль доступа пользователей к процессу загрузки операционной системы;

- контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники[36].

Стандартная загрузка операционной системы представлена на рисунке 2.7 и выполняется следующим образом:

- при включении компьютера управление передается программе BIOS, размещенной в микросхеме ПЗУ системной платы;

- BIOS выполняет тестирование работоспособности аппаратных элементов компьютера (POST-процедуры);

- в процессе окончания тестирования производится проверка наличия дополнительных BIOS, размещенных на платах расширениях (например, на определенных видеокартах, сетевых карта). При наличии дополнительных BIOS управление передается им;

- поиск загрузочного устройства на основании данных энергозависимой памяти CMOS;

- загрузка части ОС с загрузочного устройства в оперативную память и передача управления ей.

Основным инструментом обеспечения степени доверия к загрузке ОС стандартным образом является установка пароля на уровне BIOS, недостатком которой является наличие только двух пользователей (обычного и суперпользователя). Также существует различные способы сброса данного пароля:

- на современных материнских платах присутствует специальные перемычки или кнопка «Clear CMOS» для сброса пароля и настроек BIOS;

- временное удаление элемента питания CMOS на 15-30 минут;

Часто пароли для ноутбуков хранятся в специальной энергонезависимой памяти EEPROM. В этом случае для сброса пароля используют следующие подходы: прошивка EEPROM на программаторе или подборка мастер-пароля - универсального кода, подходящего к конкретной марке ноутбука[37]. Еще одним недостатком является отсутствие проверки целостности аппаратно-программных средств ПК.

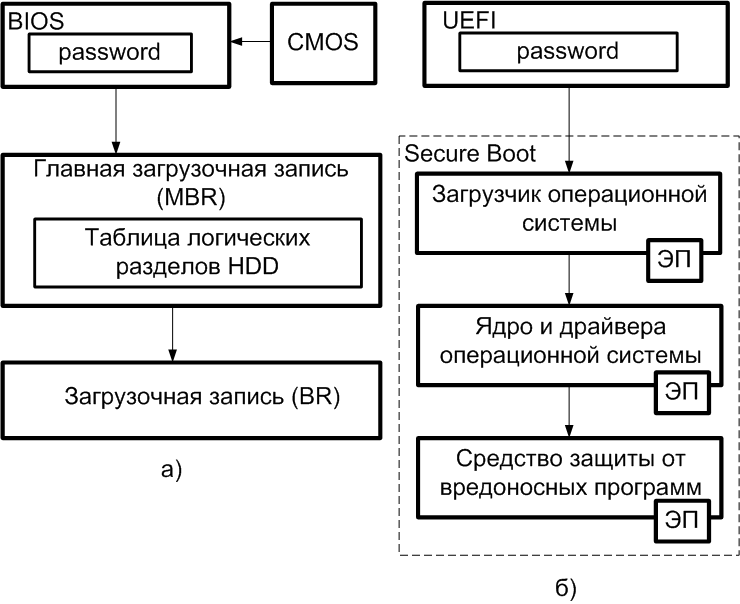


Рисунок 2.7 – Процессы загрузки компьютеров на базе BIOS и UEFI

В последние годы наблюдается тенденция использования UEFI (Unified Extensible Firmware Interface), который представляет собой замену BIOS. Это определяется ограничениями возможностей BIOS, в частности объем адресуемой памяти не превышает 1 Мб, использование только 16 и 32- разрядных команд[38]. Преимуществами UEFI перед BIOS:

-более быстрая загрузка за счет отсутствия необходимости поиска загрузчика на всех дисках;

- поддержка носителей объемом >2Тб;

- наличие собственного менеджера загрузки;

- более защищенная среда загрузки;

- графический режим конфигурации UEFI, с поддержкой графики и мыши[39].

Фактически UEFI представляет собой вполне самостоятельную ОС. Во время загрузки компьютера сперва управление передается UEFI, которая выполняет загрузочные, тестовые и рабочие сервисы, а затем уже запускается загрузка собственно операционной системы. Одним из важных достоинств данной системы является практическое отсутствие ограничения по размерам модулей драйверов и модулей, что позволять создавать дополнительные сервисы и UEFI-приложения, такие как протоколы коммуникаций, драйверы устройств, «безопасная загрузка» (secure boot, о чем в подробностях далее), низкоуровневая криптография, сетевая аутентификация[40].

На рисунке 2.7 б) представлена общая схема загрузки ПК с использованием UEFI, включающий механизм Secure Boot. Механизм «безопасной загрузки» позволяет загрузить только подписанные цифровой подписью драйвера и системные файлы ОС, что позволит проконтролировать целостность ПО. Закрытый ключ цифрового сертификата прошивается в микросхемы системной платы.

В целом, UEFI позволяет обеспечить более высокий уровень защищенности процессу загрузки ОС. Особенно перспективны работы по разработке СЗИ на данном уровне. Но при этом сохраняются ограничения подсистемы аутентификации на уровне BIOS. При этом появление хорошо унифицированного UEFI упростило разработку как легального программного обеспечения, так и вредоносного[36].

В связи с этим, в России популярны СЗИ, позволяющие обеспечить доверенную загрузку операционной системы. По типу реализации данных средств защиты различают три основных класса:

- средства доверенной загрузки уровня базовой системы ввода-вывода;

- средства доверенной загрузки уровня платы расширения;

- средства доверенной загрузки уровня загрузочной записи.

Примерами средств доверенной загрузки первого класса являются «МДЗ-ЭШЕЛОН» (НПО «Эшелон»), ALTELL TRUST («АльтЭль»). Данные средства реализуются на уровне UEFI BIOS и обладают широким функционалом:

- контроль целостности программно-аппаратных средств компьютера на основе цифровых подписей;

- поддержка аппаратных ключей аутентификации до загрузки ОС;

- возможности удаленного управления[41].

Данный класс продуктов характеризуется большими возможностями, определяемые низкими затратами на разработку модулей для UEFI BIOS и использованием практически всех аппаратных ресурсов компьютера. Степень доверия обеспечивается криптографическими методами на основе цифровых сертификатов и электронной подписи, которые позволяют контролировать целостность программного обеспечения UEFI и модулей доверенной загрузки. При этом данные средства ДЗ считаются относительно дешевыми, так как не нужно приобретать плату расширения. Это обуславливает популярность данного подхода для мобильных устройств, для которых отсутствуют аппаратные МДЗ.

К основным недостаткам к средствам ДЗ уровня базовой системы ввода-вывода являются:

- поддерживаются не все системные платы. При выборе СЗИ необходимо уточнить список поддерживаемых аппаратных средств;

- отсутствуют специальные дополнительные функции, такие как защита от ПЭМИН, аппаратного генератора случайных чисел.

Примерами средств доверенной загрузки уровня плат расширения являются ПАК Соболь («Код Безопасности»), АПМДЗ «КРИПТОН-ЗАМОК» («Анкад»), АПМДЗ "Максим-М1" (НПО «РусБИТех»). На рисунке 2.8 представлена обобщенная схема аппаратного модуля доверенной загрузки на основе платы расширения.

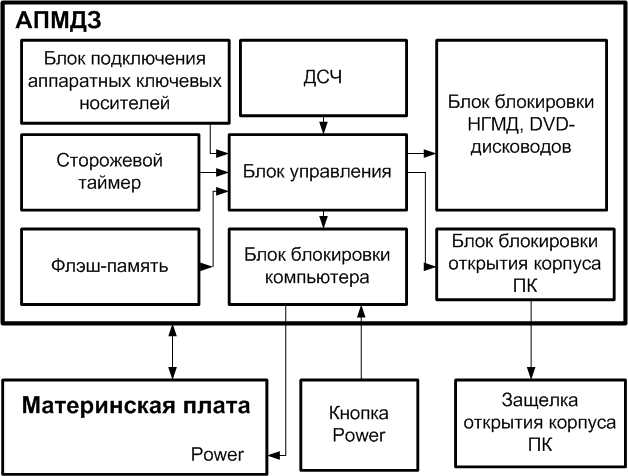


Рисунок 2.8 – Обобщенная структурная схема модуля доверенной загрузки на основе платы расширения

Принцип работы АПМДЗ заключается в следующем: после завершения POST-процедур BIOS сканирует области модулей расширений в поиска дополнительных модулей. При нахождении расширения BIOS передается ему управление.

Аппаратно-программный модуль доверенной загрузки реализует все типовые задачи: процедуры аутентификации до загрузки ОС, контроль целостности аппаратно-программных средств ПК. Отличительными особенностями данного класса СЗИ являются:

- аппаратный датчик случайных чисел, позволяющий формировать корректные сеансовые пароли;

- хранение журнала событий ИБ в энергонезависимой памяти на плате;

- аппаратные ключевые носители подключаются непосредственно к плате, что позволяет избежать раскрытия паролей пользователей вследствие возможного наличия различных видов закладок;

- наличие сторожевого таймера, который блокирует ПК при превышении интервала времени ожидания аутентификации пользователя;

- возможности блокировки на аппаратном уровне жестких дисков, дисководов;

- возможность блокировки компьютера при несанкционированном открытии корпуса ПК.

Блокировка компьютера аппаратными модулями доверенной загрузки часто осуществляется подачей сигналов сброса или питания (RESET или POWER) на системную плату. Для этого кабель от кнопки POWER\RESET компьютера подсоединяется к системной плате через АПМДЗ.

Основными достоинствами данного класса решений по доверенной загрузке является выполнение большинства функций средствами самой платы, в частности, проверки ключевых носителей. Также преимуществом является возможность блокировки ряда элементов ПК на аппаратном уровне, существует возможности контроля открытия корпуса компьютера.

Несмотря на то, что существуют модификации АПМДЗ для различных интерфейсов ПК (PCI, PCI-Express), ограничены возможности использования данного класса для мобильных устройств, ноутбуков. При выборе модулей доверенной загрузки на основе платы расширений необходимо учитывать совместимость с версиями BIOS системной платы. Решения АПМДЗ характеризуются ограниченным функционалом, определяющимся невысокими возможностями вычислительных ресурсов, в частности, небольшим объемом энергонезависимой памяти для хранения журнала безопасности. В связи с этим, данные решения взаимодействуют с программными средствами защиты для реализации расширенных возможностей. Таким примером является совместимость решения ПАК «Соболь» с СЗИ «Secret Net».

К средствам доверенной загрузки уровня загрузочной записи относятся такие решения как «Dallas Lock», «Страж NT». Основная идея заключается в модификации главной загрузочной записи MBR жесткого диска ПК. При загрузке компьютера BIOS передает управление модифицированной MBR, которая запускает выполнение код СЗИ. При успешном прохождении аутентификации пользователя, контроля целостности аппаратно-программных средств ПК и системных файлов управление передается загрузчику ОС.

Для повышения уровня защищенности необходимо настроить в BIOS загрузку операционной системы только с жесткого диска и установить пароль на изменение её параметров. Ряд СЗИ данного класса выполняют дополнительно прозрачное шифрование всего или части диска для защиты от попыток чтения конфиденциальных данных в результате загрузки со съемных носителей или подключении накопителя к другому компьютеру.

Основным достоинством решений данного класса является относительно низкая стоимость и простота установки. В большинстве случаев функция доверенной загрузки является только одной из множества функций СЗИ, большинство из которых выполняются под управлением операционной системы. Это определяет ограничение возможности применения данных СЗИ для определенного класса ОС. В основном поддерживаются ОС семейства Windows.

2.5.2 Аппаратные средства аутентификации и хранения ключевой информации

Одной из важных функций СЗИ от НСД является организация аутентификации на основе аппаратных носителей ключевой информации. Это определяется тем, что в основном в операционных системах используется для аутентификации пароли, что характеризуется низкой степенью защищенности. Применение двухфакторной аутентификации на основе аппаратных носителей реализовать стандартными средствами операционной системы является сложным процессом. Например, для ОС Windows требуется включения компьютера в домен и организации инфраструктуры открытых ключей (PKI)[42]. На рынке представлено множество средств, позволяющие организовать двухфакторную аутентификацию, в частности, Rohos Logon Key[43]. Также механизм аппаратной аутентификации входит в состав практически всех отечественных СЗИ от НСД, таких как Secret Net, Страж NT, Dallas Lock. Данные средства защиты информации позволяют использовать для аутентификации пользователя различные классы аппаратных ключевых носителей, наиболее распространенными из которых являются смарт-карты, iButton, USB-токены, флэш-носители.

Для выявления характерных особенностей аппаратных средств аутентификации, определяющие области их применения, разработана с учетом обзора литературы[45] их классификация.

Существует большое многообразие аппаратных средств, используемых для аутентификации в автоматизированных системах. По типу используемому интерфейсу выделяются аппаратные ключевые носители, использующие стандартные разъемы ПК и специальные считыватели. В основном в качестве стандартного интерфейса используется USB. Активное развитие и использование мобильных устройств в рамках АС организации потребовало разработку средств аутентификации с интерфейсами MicroUSb и MicroSD.



Рисунок 2.8 – Классификация аппаратных средств аутентификации

Ряд аппаратных ключей, которые изначально не предназначались для использования в АС, подключаются к компьютеру через специальные считыватели. Примерами таких устройств являются считыватели ключей iButton, карт-ридеры смарт-карт, RFID-считыватели радиометок. Особую группу представляют аппаратные средства генерации одноразовых паролей, которые визуально отображают ключевую информацию. К данному классу также можно отнести сотовые телефонные, позволяющие просмотреть одноразовый пароль из SMS-сообщений.

Для повышения уровня защищенности информационной системы аппаратные средства аутентификации используют несколько факторов аутентификации. В простейшем случае, используется один аутентифицирующий фактор. Например, часто в розничной торговли для идентификации и аутентификации используется штрих-код. Идея данного способа заключается в том, что человеку тяжело декодировать данный код. К данному классу устройств относятся простейшие модели ключей iButton, использующие в качестве ключевой информации идентификационный номер устройства, карты с магнитной полосой, средства радиочастотной идентификации, идентификаторы логических дисков USB-флэш-памяти. К недостаткам можно отнести относительную сложность изменения ключевого кода в случае её компрометации, требующие либо использования специальных программаторов, либо перевыпуск аппаратного носителя. Также недостатком подобных средств аутентификации является наличие у злоумышленника возможности воспользоваться утерянными или украденными устройствами. Для защиты от подобных угроз в аппаратных токенах используется дополнительный фактор – PIN-код. Для получения доступа к ИС необходимо как наличие самого аппаратного носителя, так и знание PIN-кода.

В связи с тем, что многие пользователи не меняют стандартный PIN-код токена или небрежное его хранение приводит к необходимости использования дополнительного фактора – биометрического. Это позволяет реализовать принцип неотчуждаемости носителя от владельца и обеспечить факт присутствия пользователя. Примером подобного решения является продукт фирмы «Алладин» JaCarta PKI/BIO[46].

Стойкость системы аутентификации на основе отпечатков пальцев определяется защищенностью хранилища контрольных шаблонов и подсистемы сравнения. По биометрические системы доступа делятся на три основных класса:

- Match –on-Server- сравнение шаблонов производится на сервере, там же хранятся в зашифрованном виде контрольные шаблоны;

- Match-on-PC – сравнение и хранение шаблонов осуществляется на рабочей станции;

- Match-on-Card - сравнение и хранение шаблонов осуществляется в защищенной памяти смарт-карты[47]. К данному классу устройств относятся решение JaCarta PKI/BIO, в которой биометрические данные используются для получения доступа к секретным данным в памяти смарт-карты.

2.5.3 Замкнутая программная среда

Одним из важных методов защиты от НСД к информации является организация замкнутой программной среды (ЗПС). Механизм обеспечения замкнутости программной среды предназначен для локализации программного обеспечения на компьютере (системного, функционального и прикладного ПО) и обеспечение невозможности запуска пользователем несанкционированного процесса (программы)[48].

ЗПС позволяет противодействовать скрытым угрозам ИБ за счет ограничения запуска несанкционированного программного обеспечения. Данный механизм защиты используются для защиты:

- от вредоносного ПО, вирусов, различных видов червей;

- от утечки информации по скрытым каналам связи.

Причем данный механизм позволяет защитить от угрозы как преднамеренного использования вредоносного ПО, так и непреднамеренного. Особенно актуальна ЗПС для защиты от новых видов атак, для которых еще не разработаны сигнатуры. В связи с тем, что большинство инцидентов информационной безопасности связано с инсайдерами, замкнутая программная среда позволяет ограничить возможности по запуску специализированных вредоносных программ.

Таким образом, организация замкнутой программной среды является важнейшим элементы защиты от НСД к информации, позволяющая значительно ограничить возможности злоумышленника. Кроме того, системы разграничения доступа современных ОС не могут корректно реализовывать разграничение доступа к ресурсам системы из-за того, что процессы пользователя могут вызывать системные процессы, обладающие более высокими уровнями полномочий, либо использовать низкоуровневые команды, минуя операционную систему.

Основными способами реализации замкнутой программной среды являются:

- создание списка исполняемых файлов;

- заданием разрешенных каталогов исполняемых файлов.

В первом случае создается для каждого пользователя или группы пользователей списка исполняемых файлов, которые им разрешены запускать. В качестве исполняемых файлов обычно рассматриваются не только файлы с расширениями \*.exe, но и другие, имеющие установленные флаги на выполнение. Для операционной системы Windows это файлы с такими разрешениями, как \*.dll, \*.sys, \*scr.

Корректность функционирования подсистемы организации ЗПС определяется надежностью механизма предотвращения модификации списка разрешенных процессов и контроля запуска программ. Для обеспечения корректности замкнутой программной среды необходимо обеспечить следующие требования[48]:

- исполняемый файл должен быть задан с указанием его полного пути, что предотвращает возможность запуска несанкционированного процесса с таким же именем из другого места;

- пользователю должен быть запрещен запуск программ с внешних устройств ввода (локальных и общих — разделяемых в сети), а также из общих папок (разделяемых в сети файловых объектов), т.к. иначе невозможно противодействовать запуску несанкционированной программы пользователя с полнопутевым именем легальной программы;

-пользователю должен быть задан список санкционированных для его запуска исполняемых файлов, к которым ему должен быть разрешен доступ «на исполнение». Ко всем другим файловым объектам пользователю должен быть запрещен доступ «на исполнение»;

- пользователю должен быть запрещен доступ «на запись» и «модификацию» к исполняемым файлам. В противном случае он сможет подменить санкционированный файл другого пользователя. Особенно это критично по отношению к системным процессам, поскольку нельзя допускать, чтобы пользователь мог подменить его собственным несанкционированным процессом.

Основным недостатком реализации ЗПС на основе создания списка разрешенных исполняемых файлов является сложность администрирования, определяющаяся необходимость указывать все разрешенные пользователю процессы, включая и порожденные уже разрешенными. Например, для разрешения работы приложений Microsoft Word необходимо разрешить запуск не только файла WindWord.exe, но и множества библиотек в виде dll. Вследствие этого, списки разрешенных процессов становятся большими и увеличивают вычислительную нагрузку на систему.

При организации замкнутой программной среды посредством задания каталогов исполняемых файлов для каждого пользователя определяются области дискового пространства (папки), откуда разрешен запуск программ. Для выбранного каталога должны быть установлены права доступа на «Исполнение», а также запреты на запись и модификацию с целью, чтобы предотвратить копирование не разрешенных программ и их изменение.

Таким образом, основными требованиями для организации ЗПС на основе задания каталога для разрешенных программ являются:

- для каждого пользователя определяется каталог, откуда разрешается запуск программ. Для данного каталога разрешается операция «Исполнение» и запрещаются «Запись» и «Модификация»;

- для всех остальных каталогов, включая на внешних носителях, сетевых ресурсах должен быть установлен запрет на исполнение программ;

- к системным дискам и каталогам, а также к каталогам с исполняемыми файлами других пользователей должны быть запрещены права доступа «Запись» и «Модификация».

Достоинством данного способа реализации ЗПС является относительное упрощение настройки и администрирования.

Во многих средствах защиты информации от НСД, реализующих механизм замкнутой программной среды есть два режимы работы: мягкий и жесткий. Первый режим используется для автоматизации процесса сбора данных о разрешенных для запуска процессов. В данном режиме запуск всех установленных программ разрешен, но при этом все запущенные в процессе работы пользователя исполняемые файлы фиксируются в журнале событий. На основе этих данных определяются списки санкционированных процессов. Фактически на данном этапе не включен режим замкнутой программной среды. При этом необходимо учитывать, что ряд программ загружают библиотеки не только при старте, но и в процессе работы. В связи с этим, в мягком режиме работы нужно не только запускать приложения, но требуется еще выполнять на них типовые операции. В жестком режиме работы все не разрешенные процессы блокируются, и факт события фиксируются в журналах.

2.5.4 Подсистема регистрации и учета

Важным элементом системы защиты информации от НСД, согласно руководящему документу является подсистема регистрации и учета событий ИБ. Под регистрацией событий ИБ в данной работе будет пониматься фиксация в журнале событий ИБ, которые могут представлять опасность для АС[49]. В свою очередь событие ИБ определяется как идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью[50].

Подсистема регистрации и учета предназначена для решения следующих основных задач:

- контроль корректности работы механизмов защиты информации;

- расследование инцидентов ИБ;

- предупреждение компьютерных преступлений.

Для обеспечения высокой степени объективности и доверия к системе регистрации событий необходимо выполнить следующие требования:

- только сама система защиты может добавлять записи в журнал;

- ни один субъект доступа, в том числе сама система защиты, не имеет возможности редактировать отдельные записи;

- в АС кроме администраторов, регистрирующих пользователей и устанавливающих права доступа, выделяется дополнительная категория — аудиторы;

- только аудиторы могут просматривать журнал;

- только аудиторы могут очищать журнал;

- полномочия администратора и аудитора в рамках одного сеанса несовместимы;

- при переполнении журнала система защиты аварийно завершает работу[49, 19].

Современные ОС содержат внутренние механизмы регистрации основных событий системы. Например, операционные системы семейства Windows позволяют настроить параметры для регистрации событий следующих типов: входа в систему, доступа к объектам (файлы, папки, принтеры, разделы системного реестра), изменения привилегий, системных событий, управления учетными записями. Информация о событиях протоколируются в специальных журналах ОС, например, в журналах системы, приложений, безопасности. В целом, возможности подсистема регистрации и учета ОС Windows достаточна для решения основных задач ИБ, имеются средства просмотра записей и их фильтрации.

На рисунке 2.9 представлена классификация систем регистрации событий.



Рисунок 2.9 – Классификация систем регистраций событий

Применение внешних средств регистрации событий, например, Secret Net, Dallas Lock, Страж NT позволяет использовать более расширенные возможности протоколирования. В частности, данные средства позволяют фиксировать события полномочной системы управления доступом, контроля и извлечения устройств, межсетевого экрана и средств обнаружения вторжений. Особое место занимает механизм теневого копирования, обеспечивающий копирование информации, которую пользователь записывает на сменные или сетевые накопители или отправляет на печать, в специальную папку на локальном жестком диске для последующего анализа[51]. Также в ряде решений реализуются возможность установки штампа на все распечатываемые документы, позволяющий зафиксировать «механически» уровень конфиденциальности на бумаге.

При использовании любых решений для регистрации необходимо определить политику аудита- совокупность правил, определяющих протоколирование событий в журналах. При этом необходимо выбрать оптимальное количество регистрируемых событий:

- малое количество событий может привести к пропуску важных событий информационной безопасности;

- избыточное количество протоколируемых событий приводит к переполнению журналов событий и увеличения вычислительной нагрузки.

**3 Аппаратные средства хранения ключевой информации**

**3.1 Идентификаторы iButton**

Аппаратные идентификаторы iButton (раньше назывался Touch Memory) были разработаны в 1991 году фирмой Dallas Semiconductor. Представляют собой микросхему, размещенную в герметичном металлическом корпусе (рисунок 3.1).

Рисунок 3.1 – Электронный ключ iButton

Для обмена данными между iButton и считывателем используется интерфейс 1-Wire. Передача данных осуществляется при прикосновении корпуса электронного ключа к считывателю за время не более 5мс[52]. Основными достоинствами устройств данного класса являются невысокая стоимость, высокая степень механической и электромагнитной защищенности.

На рисунке 3.2 представлена обобщенная структурная схема аппаратного идентификатора iButton.

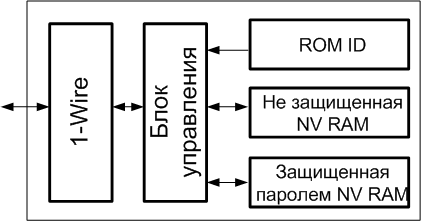


Рисунок 3.2 – Структурная схема электронного ключа iButton

Основными элементами ключей семейства iButton являются:

- постоянное запоминающее устройство, хранящее 64-битный уникальный идентификатор для каждого устройства. Данный номер наносится производителем при изготовлении;

- незащищенное энергонезависимое ОЗУ (NV RAM);

- защищенное энергонезависимое ОЗУ (NV RAM).

Отдельные модели электронных ключей дополнительно содержат часы реального времени (для DS1994), литиевую батарею (DS1992-DS1996), позволяющую сохранять в ОЗУ данные в течение 10 лет, криптографический SHA-процессор (для DS1963S).

Особенностью аппаратных ключей iButton является «паразитное питание» по однопроводному интерфейсу 1-Wire, заключающийся в том, что питание устройства осуществляется по тем же линиям, что и данные. При наличии высокого уровня сигнала на линии данных заряжается внутренний конденсатор, который питает устройство при отсутствии напряжения.

В общем, все устройства iButton можно рассматривать мобильные элементы памяти, которые передают данные при соприкосновении. В связи появлением новых моделей устройств менялись и виды используемой памяти. Тип памяти устройства определяет его область применения. По виду памяти различают следующие классы устройств iButton:

* 64-битный ROM, содержащий уникальный номер устройства;
* статическая память (NV RAM) размером от 1 до 64 Кбит, позволяющий выполнять операции чтения и записи. Данные устройства используются для задач, в рамках которых требуется частое изменение данных;
* однократно программируемая память (EPROM);

- электрически стираемое перепрограммируемое ПЗУ (EEPROM). Данные устройства дешевле, чем с памятью NV RAM, но поддерживают меньшее количество записей[53].

Устройства iButton находят широкое применение в областях с повышенным уровнем воздействия внешней среды и тяжелыми условиями эксплуатации, где традиционные карточки или устройства для считывания с них информации могут быстро выйти из строя. В зависимости от категории защищенности объекта, применяются различные типы iButton. Так, для ограничения доступа в подъезды жилых домов, где не предъявляются повышенные требования к системам ограничения доступа, используют самые дешевые iButton DS1990[54]. Для систем, в которых необходимо контролировать время доступа, может быть использовано устройство DS1994L. Емкость времени данного электронного ключа составляет 136 лет.

Наиболее популярными областями применения ключей iButton являются:

- системы контроля доступа к помещениям, оборудованию и устройствам;

- системы компьютерной безопасности;

- систем организации платежей на общественном транспорте;

- средство доставки электронных квитанций;

- инструмент контроля патрульных служб[55].

Основным недостатком аппаратных ключей iButton являются:

- необходимость установки считывателя для компьютерных систем;

- надежность срабатывания устройства зависит от точности соприкосновения с считывателем;

- относительно небольшой объем памяти.

**3.2 Система электронных платежей на основе iButton DS1963S**

Одной из самых защищенных моделей устройств iButton является DS1963S, использующийся в системах электронной оплаты. На сегодняшний день активно используются электронные деньги благодаря таким характеристикам, как высокая портативность, низкая стоимость создания. По типу реализации системы электронных платежей делятся на два основных класса: он-лайн и офф-лайн. В первом случае все операции с электронными деньгами осуществляются по сети Интернет и фиксируются в платежной системе. Во втором случае производится выгрузка данных о состоянии счета на устройства с памятью, например, смарт-карт. Это позволяет производить операции автономно без подключения непосредственно к центру обработки состояния счета. К данному классу относится устройство DS1963S, в котором реализованы ряд архитектурных решений, направленных на повышение уровня защищенности.

Невысокая стоимость DS1963S, устойчивость к негативным воздействия окружающей среды, обеспечиваемый достаточно высокий уровень информационной безопасности определило широкое применение в таких платежных системах, как автоматы продажи товаров, АЗС, общественный транспорт.

Для электронных платежных систем типа офф-лайн характерны следующие виды угроз:

- подделка устройства хранения информации о состоянии счета;

- копирование информации с оригинального устройства на дублирующие;

- преждевременное завершение операции оплаты товара или услуги с целью блокирования изменения остатка на счете в памяти устройства.

Для обеспечения высокого уровня защищенности платежной системы используются операции криптографического преобразования. Наиболее популярным является применение различных видов шифрования. Несмотря на достоинства шифрования необходимо отметить следующие недостатки:

- значительные временные затраты на выполнение криптографического преобразования, что требует использование дорогих и высокопроизводительных устройств;

- при перехвате злоумышленником секретного ключа возможность расшифровки конфиденциальной информации.

Альтернативой является использование хеш-функций, что реализовано в DS1963S. При рассмотрении вопроса организации системы электронных денег на базе ключей iButton важным понятием является код идентификации сообщения, схема формирования которого представлена на рисунке 3.3.

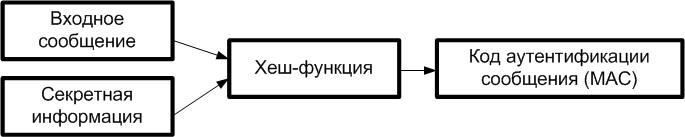


Рисунок 3.3 –Схема генерации кода аутентификации сообщения

MAC представляет собой хеш-значение, вычисленное по алгоритму SHA-1. Данный алгоритм описан в стандарте ISO/IEC 10118-3. Только участник информационного взаимодействия, который знает секретный ключ, может сгенерировать правильное значение хеш-функции. В системах использующих электронные деньги на базе устройства DS1963S данный MAC используется также для контроля целостности баланса.

На рисунке 3.4 представлена обобщенная схема DS1963S, использующаяся в системах оплаты с электронными деньгами.



Рисунок 3.4 –Структурная схема устройств в системе оплаты на базе DS1963S

Ключ аутентификации токена формируется на этапе инициализации в результате вычисления хеширования идентификатора устройства и главного ключа модуля контроля.

Типовая схема потоков систем оплаты на основе ключей iButton DS1963S представлена на рисунке 3.5.

Рисунок 3.5 – Типовая схема информационных потоков для DS1963S[56]

При начале взаимодействия модуль контроля сервиса генерирует случайное число, которое первоначально сохраняется в памяти ключа iButton. В ответ, токен генерирует MAC аутентификации на основе следующих данных:

- случайное число, полученное от модуля контроля;

- ***Rom ID***;

- ключ аутентификации токена.

Данное хеш-значение проверяется модулем контроля и проверяется подлинность аппаратного ключа. Далее токен передает данные о балансе, код транзакции, сигнатуру данных сервиса и значение счетчика количества операций записи в страницу памяти. Контролирующая подсистема сверяет полученное значение сигнатуры баланса с рассчитанным значением хеша над следующими данными: значение баланса, код транзакции и счетчика количества операций записи в страницу памяти, главный ключ для подписи данных. Данная операция позволяет удостовериться, что данные баланса не были модифицированы злоумышленником.

Счетчик количества операций записи изменяется автоматически и нет возможности его модифицировать штатными операциями. Данная функция используется для предотвращения дублирования ключа. Код транзакции позволяет защитить от атак, когда злоумышленник начинает покупку товара на автомате ***А***, затем прерывает операцию и переходит к автомату ***B***. После покупки товара на автомате B возвращается к устройству ***A*** и завершает операцию. Если бы токен и модуль контроля не проверяли бы значение счетчика, то злоумышленник потенциально мог бы получить 2 товара, при этом со счета списалось бы только одна сумма[57]. Фактически код транзакции – это случайное число генерируемое модулем контроля сервиса (МКС).

После проверки целостности данных о балансе производится списывание денег с устройства DS1963S следующим образом:

- производится изменение баланса на сумму товара МКС;

-подсчитывается новое значение MAC, используя новый баланс, счетчик, код транзакции и главный ключ для подписи;

- новое значение баланса и сигнатуры данных записывается в память аппаратного ключа.

Также необходимо отметить, что использование специализированного процессора позволяет выполнять операции хеширования за короткий интервал времени, что позволяет снизить вероятность воздействия злоумышленника на канал передачи данных. При этом все вычисления производятся внутри устройства без передачи вне секретных ключей.

Таким образом, устройства iButton DS1963S обеспечивают высокий уровень защищенности благодаря таким достоинствам:

- позволяет осуществить аутентификацию пользователя;

- надежно хранит в памяти баланс счета;

- определяет модификацию злоумышленником баланса в памяти устройства;

- имеет физически защищенный стальной контейнер;

- высокая трудоемкость вскрытия устройства;

- быстрая криптографическая подсистема[57].

**3.3 Смарт-карты**

Смарт-карта - это пластиковая карта со встроенным микропроцессором, выполняющим функции контроля доступа к памяти и функции криптографического преобразования. Данные устройства позволяют осуществлять не только надежное хранение информации, но и позволяют осуществлять дополнительную её обработку. Область применения смарт-карт характеризуется большим многообразием: банковская система, сотовая связь, цифровое телевидение, электронные кошельки, физический доступ к помещениям, доступ к компьютерным системам. Существуют различные виды смарт-карт, классификация которых представлена на рисунке 3.6.



Рисунок 3.6 –Классификация смарт-карт

Карты памяти используются для хранения небольшого объема данных и не выполняют никаких дополнительных вычислительных операций. Выделяются в отдельную группу устройства, у которых есть механизмы защиты от несанкционированной записи и чтения данных из памяти. Данные карты часто используются для удостоверения личности в системах контроля доступа.

Другой популярной группой являются смарт-карты для хранения состояния счета. Например, карты для оплаты телефонных разговоров на таксофонах. В данных картах реализуются механизмы, предотвращающие возможности записи данных в ячейки памяти. Массивы памяти работают как декрементные (вычитающие) счетчики, уменьшающие значение баланса. При обнулении значения счетчика, карта становится бесполезной[58].

Интеллектуальные карты с микропроцессором позволяют не только хранить секретные данные, но и выполнять сложные криптографические преобразования. Также данные устройства могут содержать аппаратные генераторы случайных чисел, усиленную защиту от физической атаки. Данные возможности позволяют использовать данные карты для построения защищенных информационных систем. Интеллектуальные карты используются для хранения цифровых сертификатов, шифрования данных, формирования электронных подписей и удаленной аутентификации. Реализация большого количества функций для данных устройств приводит к увеличению их стоимости.

Большинство типов смарт-карт являются контактными. При установке карты в считыватель контакты чипа соприкасаются с электронными коннекторами, через которые происходит обмен данными. Питание на смарт-карту передается через считыватель. Популярность применения смарт-карт для компьютерных систем обусловило появление устройств с USB-интерфейсом. Данные карты для подключения к компьютеру не требуют использования специальных считывателей. Наиболее популярными устройствами данного класса в России являются Rutoken и eToken. Недостатком данных устройств являются сбои в работе в результате износа контактов вследствие физического воздействия. Негативно воздействуют и прерывание контактов при вибрации мобильных устройств, использующих смарт-карты. Так как контакты смарт-карты связаны с внутренней микросхемой, то возможно воздействие статического электричества высокого напряжения, что приведет к отказу устройства. Решением подобных проблем является использование бесконтактных устройств. Дополнительным преимуществом данного класса устройств является возможность использования их на расстоянии до нескольких метров. Конечно, терминалы считывания для таких карт являются более сложными и дорогими.

Общая структурная схема интеллектуальных смарт-карт представлена на рисунке 3.7.



Рисунок 3.7 – Структурная схема смарт-карты

Основу микросхемы смарт-карты составляет процессор, выполняющий основные вычисления. Для реализации сложных криптографических систем, виртуальных машин на базе смарт-карт требуется высокая производительность процессоров. Для реализации сложных алгоритмов криптографических преобразований часто используются специализированные сопроцессоры, что позволяет сократить время решения подобных задач. При этом процессор подготавливает данные и передает для сопроцессора.

В постоянное запоминающее устройство записывается операционная система и программа диагностики при изготовлении чипа и не может быть изменена во время жизни. EEPROM представляет энергонезависимую память микросхемы. Данные в EEPROM записываются и считываются под управлением операционной системы смарт-карты. Оперативная память RAM используется для хранения временных данных, например, стека, входных данных от подсистемы ввода/вывода данных. Блок диагностики осуществляет проверку контрольных сумм данных, записанных в различные типы памяти, осуществляется мониторинг температуры, напряжения питания. Эффективность большинства криптографических систем зависит от качества реализации генератора случайных чисел. В связи с тем, что смарт-карты часто применяются как средства шифрования, то им требуется свой собственный генератор.

Подсистема ввода-вывода может быть реализована в виде контактов с интерфейсом стандарта ISO 7618, USB-интерфейсом или бесконтактный. Для использования контактных и бесконтактных смарт-карт в компьютерной системе требуется использование считывающего устройства.

В компьютерных системах используются следующие основные схемы применения смарт-карт:

- смарт-карта используется как надежное хранилище аутентифицирующей информации. Чаще всего сохраняются закрытый ключ сертификатов. При этом все криптографические операции осуществляются на рабочей станции;

- смарт-карта используется не только для защищенного хранения секретной информации, но и выполняет криптографические операции внутри устройства. Так в смарт-карте могут выполняться операции генерации ключевой пары, шифрование данных, формирование электронной подписи.

Важным элементом защиты систем, использующих смарт-карты, является использование PIN-кода для получения доступа к устройству. Это позволяет защитить от угроз потери или кражи аппаратного носителя ключевой информации. При вводе определенного количества неправильных PIN-кодов устройство блокируется. PIN-код должен содержать от 4 до 12 символов. В большинстве устройств, в частности, USB-токенах используются цифры от 0 до 9. Многие пользователи оставляют стандартные PIN-коды устройств, что снижает степень защищенности компьютерных систем.

В следующем разделе будут рассмотрены наиболее известные решения для защиты информации на базе USB-токенов.

**3.4 USB-токены**

Наиболее популярным видом смарт-карт являются в компьютерных системах USB-токены благодаря использованию стандартного компьютерного интерфейса. На рынке представлены различные типы устройств данного класса, отличающиеся по стоимости и функциональным возможностям. Наиболее простыми USB-токенами являются устройства, предназначенные только для безопасного хранения ключевой информации.

Примером подобного устройства является решение фирмы «Актив» Рутокен Lite. Рутокен Lite можно использовать для безопасного хранения ключей шифрования и электронной подписи, паролей и других данных во встроенной защищенной памяти устройства. Применяется для авторизации в компьютерных системах и защиты персональных данных[59]. При двухфакторной аутентификации аутентификаторами являются обладание устройством и знание PIN-кода. При этом число попыток ввода PIN-кода ограничено. Основным достоинством устройств данного класса является в возможности использования длинных и сложных паролей без необходимости их запоминать: ключевая информация сохраняется в защищенной памяти устройства, доступ к которой можно получить только при вводе за заданное количество попыток PIN-кода.

При использовании данного устройства в системах выполняющие криптографические операции необходимо учитывать, что они производятся на компьютере, программное обеспечение которого может быть модифицировано, например, вирусом. В связи с этим, при применении данных устройств для шифрования, формирования электронной подписи, на рабочем компьютере должны быть предусмотрены дополнительные меры защиты, таки как СЗИ от НСД, антивирусы.

Более предпочтительно использование USB-токенов, позволяющих выполнять криптографические преобразования внутри устройства и генерировать случайные числа для формирования ключевой информации. В результате закрытые ключи не покидают устройство, что повышает уровень защищенности системы.

На рисунке 3.8 представлена структурная схема средства криптографической защиты информации на базе токена. Основным элементом является USB-токен, осуществляющий аппаратное шифрование. В перепрограммируемой памяти firmware хранится программный код библиотек, реализующие различные криптографические алгоритмы, такие как шифрование, вычисление хеш-функции, вычисление и проверка электронной подписи. В энергонезависимой памяти надежно хранится ключевая информация. Аппаратный датчик случайных чисел используется для генерирования различных видов ключей: сеансовых и долговременных. Для хранения большого объема данных используется Flash-память, защищенная PIN-кодом

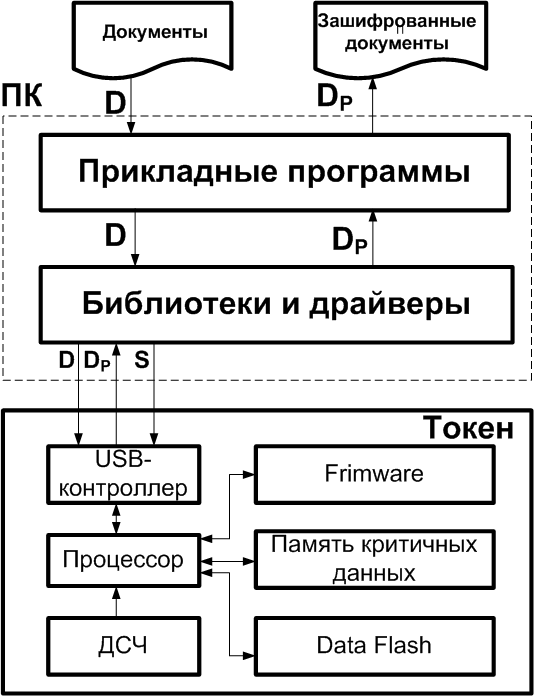


Рисунок 3.8 – Структурная схема средства криптографической защиты информации на базе токена

Общий алгоритм выполнения криптографического преобразования над данными с использованием интеллектуальных токенов имеет следующий вид:

- ввод пользователем PIN-кода USB-токена ***S***;

- передача данных ***D*** из компьютера USB-токену;

- выполнение криптографических операций токеном с использованием закрытых ключей, сгенерированных аппаратным ДСЧ и хранимых в защищенной памяти;

- передача результата преобразования ***DP*** в компьютер из токена.

Примерами устройств данного типа являются Рутокен S, Рутокен ЭЦП, eToken ГОСТ и другие. Данные токены позволяют защитить от перехвата ключевой информации, модификации и имитации криптографического преобразования над данными. Практически невозможно вмешательство в протекание процессов аутентификации, шифрования или выработки/проверки ЭЦП и их фальсификация. Это значит, что ни во время сеанса работы, ни после отключения в память компьютера не попадает ключевая информация, и она не может быть перехвачена или восстановлена злоумышленником[60]. Но при этом не защищают от передачи не корректных данных в систему криптографической защиты информации. Например, пользователь на экране может видеть одну информацию, а перед подписыванием документа или шифрованием вредоносная программа может подменить данные и только потом передать токену.

Производители USB-токенов добавляют дополнительные функциональные возможности данным устройствам. В частности, производятся токены, интегрирующие возможности смарт-карты и управляемой Flash-памяти. Общая структурная данного типа решения представлена на рисунке 3.9.

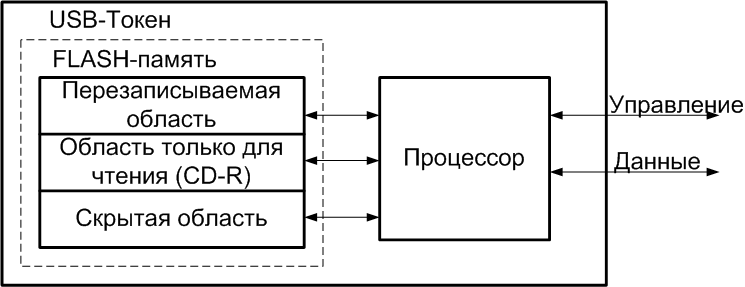


Рисунок 3.9 – Структурная схема USB-токена с Flash-памятью

Особенностью рассмотренного выше устройства является наличие большого объема памяти, доступ к которой обеспечивается процессором токена. Flash-память распределяется на несколько областей. Перезаписываемая область используется просто как память большого объема, который защищается PIN-кодом устройства. В устройствах предусматривается создание разделов только для чтения, в том числе, CD-ROM разделов. Дополнительно присутствует возможность создания скрытого раздела в Flash-памяти, шифрование данных[61, 62].

Основными областями применения USB-токена с Flash-памятью являются:

- автозапуск приложений, тиражирование и автоматическая установка программ;

- безопасное хранение и транспортировка данных;

- доверенная загрузка рабочих станций, серверов, терминальных клиентов.

Для работы с государственными информационными системами часто требуется использовать специализированное программное обеспечение, устанавливать доверенные сертификаты, осуществлять настройку параметров ПО, например, браузера. В связи с этим, существует необходимость в средствах, позволяющих автоматизировать процесс установки и настройки программного обеспечения рабочего пользователя. Комплект необходимого программного обеспечения может быть размещен в CD-ROM разделе и настроен на автозапуск. При этом токен обеспечивает защиту от НСД к данным при потере устройства за счет использования PIN-кода. Использование для хранения установщиков программ и статичных данных раздела только для чтения защищает от возможной модификации со стороны вредоносного ПО.

Также USB-токен с Flash-памятью используются для доверенной загрузки операционной системы. При этом для аутентификации могут использоваться ключи, сертификаты, сохраненные в памяти токена. Примерами подобных устройств являются следующие решения: Рутокен ЭЦП 2.0 Flash, eToken NG-Flash, Jacarta Flash.

**3.5 USB-токены с биометрической идентификацией**

Многие пользователи часто передают другим сотрудникам свои аппаратные ключи и сообщают PIN-коды. Такой подход увеличивает риск информационной безопасности предприятия, что обуславливает необходимость обеспечения неотчуждаемости токена от его владельца. Для решения данной задачи были разработаны USB-токены, позволяющие дополнительно осуществлять биометрическую аутентификацию. На базе данных устройств может быть построена система, реализующая трехфакторную аутентификацию: обладание электронным ключом, PIN-код и биометрический параметр. Подобное решение представлено компанией «Алладин» - JaCarta PKI/BIO[47]. На рисунке 3.10 представлена функциональная схема системы аутентификации с использованием USB-токена с технологией Match-on-Card.

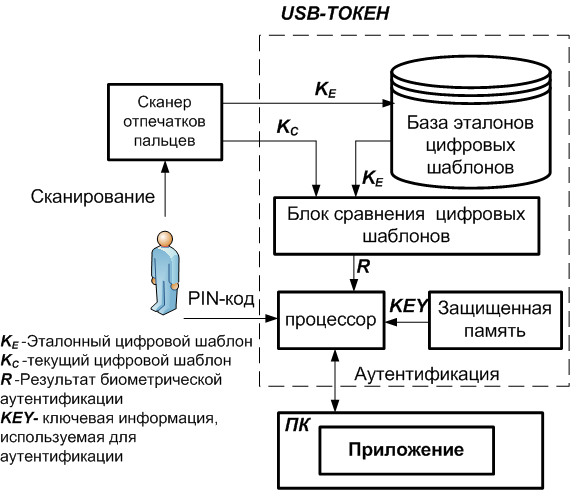


Рисунок 3.10 – Структурная схема системы аутентификации с использованием технологии Match-on-Card

Сканер отпечатков формирует цифровой шаблон, содержащий информацию о ключевых признаках отпечатка пальца, достаточных для идентификации с приемлемой точностью. При этом в системе не сохраняются и не обрабатываются биометрические персональные данные, так как по цифровому шаблону невозможно восстановить отпечаток пальца. Успешная биометрическая аутентификация и правильно введенный PIN-код позволяют получить доступ к ключевой информации, используемой, например, для аутентификации.

Достоинствами данной системы являются:

- сравнение и хранение цифровых шаблонов осуществляется только в электронном ключе, что практически делает не возможным воздействия на процесс аутентификации;

- отсутствие необходимости в централизованной базе данных для хранения отпечатков пальцев всех пользователей;

- обеспечивается принцип неотчуждаемости носителя от владельца;

- достаточно приемлемая стоимость и удобство работы.

**3.6 Электронные ключи с поддержкой открытого протокола двухфакторной аутентификации U2F**

Высокий уровень информатизации, приводящий к увеличению числа предоставляемых услуг в электронном виде, определяет высокие требования к системе аутентификации Web-сервисов. Последние годы прослеживается использование двухфакторной аутентификации для входа в различные WEB-сайты, в частности, использующие различные токены, одноразовые SMS-пароли. Использование токенов требуют установки драйверов, специальных плагинов, что создает сложности для обычных пользователей. Применение OTP на основе SMS характеризуется относительно невысоким уровнем ИБ в связи с существованием следующих угроз:

- низкий уровень защищенности сетей сотовых операторов, что приводит к высокому риску возможности перехвата входящих SMS[63];

- возможность перевыпуска SIM-карты по поддельным документам.

Основными недостатками существующих систем двухфакторной аутентификации (2FA) Web-сервисов являются:

- большинство 2FA решения уязвимы к MITM (men in the middle) атакам, и соответственно фишингу;

- стоимость. Криптографические токены, отлично себя зарекомендовавшие с точки зрения безопасности — достаточно недешевое удовольствие. Их покупка ложится на плечи конечных пользователей, редкий сервис берет их оплату и доставку пользователю на себя. Даже отправка SMS стоит денег. Таким образом, внедрение и использование 2FA могут позволить себе далеко не все.

- совместимость. Далеко не все операционные системы имеют в своем составе драйвера для работы криптографических токенов;

- удобство использования. Пользователям лень вводить одноразовые пароли. Разблокируй экран телефона, открой сообщение или OTP программу, прочитай код, введи его, ошибись, повтори все сначала — это стандартный алгоритм взаимодействия пользователя и двухфакторной аутентификации[64].

В связи с этим, был организован альянс FIDO (Fast IDentity Online) для разработки стандартов удобной и безопасной аутентификации в Интернете. FIDO представил спецификации 2 протоколов : U2F (Universal Second Factor) — универсальный протокол двухфакторной аутентификации, UAF (Universal Authentication Framework) — универсальный протокол для биометрической аутентификации [65,66]. Первый протокол описывает в основном взаимодействие клиентского приложения с U2F-устройством, использующимся для аутентификации. Структурная схема системы аутентификации в Интернете на основе U2F представлена на рисунке 3.11.

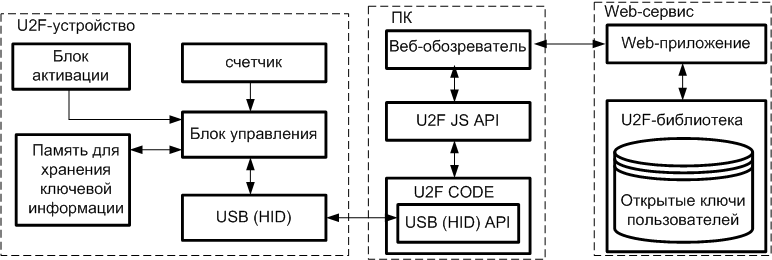


Рисунок 3.11- Система аутентификации в Интернете на основе U2F

В общем работе протокола U2F делится на два этапа: регистрация U2F-устройства и аутентификация с помощью него.

Регистрация U2F-устройства производится один раз при первом подключении из личного кабинета без привлечения администратора. Далее Web-сервер передает клиенту идентификатор приложения (AppID) и случайное число. На основе этих данных U2F-устройство при нажатии кнопки активации генерирует уникальную пару ключей (***Kpub*** открытый и ***Kpriv*** закрытый) и их идентификатор ***KeyHandle***. При этом закрытый ключ не покидает защищенную память устройства.

На рисунке 3.12 представлена схема взаимодействия элементов системы аутентификации U2F. Данная система аутентификации базируется на механизме «запрос-ответ» и использует ассиметричную криптографию. Обмен данными между браузером и web-сервером осуществляется в зашифрованном виде на основе протокола HTTPS с использованием сертификатов.

На первом этапе пользователь вводит логин и пароль. В ответ Web-сервер формирует запрос, включающий сгенерированное случайное число ***Ch***, зарегистрированный идентификатор ключей ***KeyH***  и идентификатор сервиса ***AppID***. Далее web-обозреватель добавляет к запросу доменное имя сайта URL и идентификатор сессии протокола TLS (транспортный уровень HTTPS) и передает запрос на электронное устройство U2F. На следующем шаге пользователь должен подтвердить свое присутствие, например, нажав кнопку на U2F-устройстве. В ответ электронное устройство выбирает по полученному идентификатору ***KeyH*** соответствующий закрытый ключ и формирует электронную подпись над данными полученного запроса ***С*** и значением счетчика ***Cnt***.

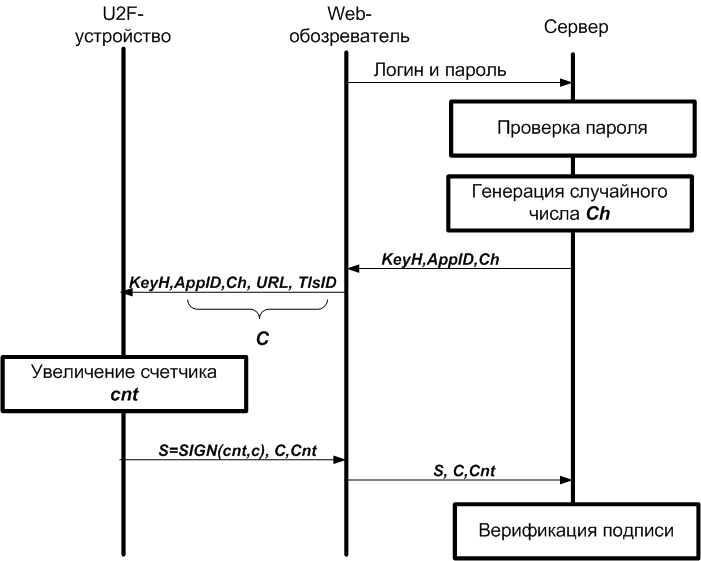


Рисунок 3.12 – Схема взаимодействия элементов системы аутентификации на основе U2F- протокола[67]

Web-сервер проверяет корректность электронной подписи ***S*** при помощи открытого ключа, сохраненного в базе данных при регистрации. При успешной проверке подписи процесс аутентификации завершается.

Основными достоинствами протокола U2F являются:

- самостоятельная регистрация пользователя. При этом не требуется PKI, удостоверяющий центра;

- защита от фишинга. Достигается за счет добавления в запрос URL сервиса, который определен в браузере, и идентификатора сессии протокола TLS. При проверке подписи сервер удостоверяется, правильное доменное имя было указано в обозревателе клиента;

- одно устройство используется для аутентификации множества сервисов. Это определяется тем, что для формирования ключевой пары устройство использует идентификатор сервиса AppID и случайное число ***Ch***. Данный механизм обеспечивает высокую степень уникальности сформированных ключей;

- защита от клонирования U2F-устройства. В электронном устройстве содержится счетчик, значение которого автоматически увеличивается при каждой операции аутентификации и регистрации. Сравнивая значение счетчика, сохраненное в базе данных сервера, и полученного от клиентского устройства можно определить копию U2F-устройства;

- защита от попыток воспользоваться электронным ключом вредоносной программой при отсутствии пользователя. Все операции регистрации и аутентификации подтверждаются нажатием специальной кнопки;

- относительно невысокая стоимость и простота устройства. Электронное устройство не является СКЗИ, что не требует наличия дополнительных сертификатов и упрощает структуру.

Дополнительно электронные устройства могут иметь цифровые сертификаты производителя, подтверждающие высокий уровень их защищенности. Сформированная U2F-устройством подпись дополнительно подписывается сертификатом. Таким образом сервер, может проверить класс устройства и отказать проводить аутентификацию с ненадежными решениями.

Примером устройства, поддерживающего U2F протокол является решение JaCarta U2F[68]. Данный протокол становится все более популярным и внедрен в таких сервисах, как GitHub, DropBox, все сервисы Google, государственных информационные системы Великобритании.

**3.6 Устройства класса TrustScreen**

Удобство работы с дистанционными системами банковского обслуживания (ДБО) обусловило их широкое распространение и привлекло внимание злоумышленников. Отсутствие высокого уровня защищенности данных систем может привести к тому, что злоумышленники переведут денежные средства на свои счета. Поэтому вопросы обеспечения защиты ДБО являются сегодня особенно актуальными.

Обобщенная структурная схема системы дистанционного банковского обслуживания представлена на рисунке 3.13.



Рисунок 3.13 – Структурная схема системы ДБО

На стороне клиента размещается специализированное программное средство, при помощи которого осуществляет дистанционные платежи. Обмен данными с информационной инфраструктурой банка используется чаще всего сеть Интернет. Для защиты канала связи между компьютером клиента и сервером ДБО либо организуется VPN-канал, либо производится шифрование на основе протокола https. Для хранения паролей используются в основном USB-токены.

Основными объектами атаки злоумышленников являются: ПК клиента и сервер ДБО. В большинстве случаев уровень защиты информационной инфраструктуры характеризуется высоким уровнем защищенности. В связи с этим, большинство атак на ДБО направлены на ПК клиента. Наиболее распространенными видами атак на клиента системы дистанционного банковского обслуживания являются:

- кража ключей цифрового сертификата с использованием вредоносного программного обеспечения. На первых этапах развития ДБО ключи хранились на дискетах, в разделах жестких дисков, в разделах реестрах в виде программных токенов, что облегчало их копирование для злоумышленника;

- несанкционированный доступ к USB-токену/ смарт-карту с использованием вредоносных программ удаленного доступа к компьютеру, удаленного доступа к USB. Кроме получения доступа злоумышленнику необходимо, чтобы электронный ключ был подключен к компьютеру и знать PIN-код устройства;

- подмена документа перед его передачей токену для подписывания. При том пользователь на экране видит искаженную информацию. При этом злоумышленником возможно использование как уязвимости системы клиент-банк, так и наличие вредоносного ПО [69].

Первый тип атаки нейтрализуется за счет использования аппаратных ключей хранения цифровых сертификатов. Для защиты от атак второго класса необходимо организовать доверенную среду. Использование средств доверенной загрузки операционной системы, контроля целостности программного обеспечения недостаточно для защиты от третьего типа атак. Например, если клиентом используется система банк-клиент на основе web-обозревателя, то возможны атаки на сам web-сервер. Кроме того необходимо отметить, что использование средств организации доверенной загрузки требуют дополнительных затрат, возможны конфликты с существующими сервисами предприятия. Все это определяет необходимость внедрения новых средств защиты информации для обеспечения требуемого уровня безопасности для ДБО.

Необходимо отметить, что в системах ДБО активно используются системы антифрода для защиты клиентов от мошенничества. В этом случае банк на основании некоторых знаниях о предыдущих операциях клиента, в целом клиентской массы, черных списков и т.п. пытается понять, насколько велик риск мошенничества по данной операции. Однако подобные системы не могут обеспечить полную безопасность[70].

Для защиты от всех трех видов рассмотренных выше атак требуется обеспечить выполнение следующих требований:

- строгая аутентификация пользователя;

- визуальный контроль подписываемых данных;

-подтверждение присутствия пользователя при формировании электронной подписи;

- формирование электронной подписи в USB-токене с использованием неизвлекаемых ключей[69].

В связи с тем, чтобы обеспечить безопасную работу в системе ДБО необходимое строгое выполнение следующих минимальных требований:

- использование только лицензионного и сертифицированного ПО (операционные системы, прикладное ПО, средства криптографической защиты информации);

- своевременное обновление программного обеспечения;

- установка и правильная настройка средств защиты информации (МСЭ, антивирусы);

- установка средств доверенной загрузки и контроля целостности программно-аппаратных средств компьютера[71].

Выполнение только данных требований требует непрерывный контроль системы защиты информации, временных и стоимостных затрат, высокий уровень профессиональных знаний сотрудников отдела ИБ. Данные условия для большинства предприятий, особенно небольших трудновыполнимы. В результате предлагается использовать следующий подход:

-исходить из того, что пользователи работают в не доверенной среде;

- для работы с системой ДБО использовать специальное доверенное устройство.

В качестве доверенного устройства используется токен с экраном, особенностью которого является то, что кроме формирования электронной подписи непосредственно в нем при помощи неизвлекаемых ключей, также на экране отображаются подписываемые данные. На рисунке 3.14 представлена схема взаимодействия элементов системы ДБО с использованием токена с экраном.



Рисунок 3.14 Схема информационных потоков системы ДБО

Для выполнения операций в системе ДБО клиент должен пройти аутентификацию с использованием токена. Уже на данном этапе проявляется преимущество токена с экраном – ввод PIN-кода для получения доступа к электронному ключу осуществляется при помощи клавиатуры доверенного устройства. Далее пользователь формирует платежное поручение при помощи прикладного ПО на компьютере клиента и отправляет документ на сервер ДБО. Сервер в ответ возвращает документ, его шаблон и идентификатор журнала операций. Шаблон представляет собой описание, какие реквизиты документа отображать на экране устройства TrusScreen. Для предотвращения модификации этого шаблона при передаче от Интернет банка до токена с экраном осуществляется формирование его электронной подписи цифровым сертификатом банка. Идентификатор журнала операций представляет собой некое случайное число, которое добавляется в запись журнала операций токена. Данный идентификатор позволит защитить от копий данных сформированных злоумышленником[70, 72].

На 5 шаге токен отображает реквизиты документа, например, получателя, номер счета, сумму и ожидает подтверждения от пользователя в виде PIN-кода, введенного на клавиатуре устройства. На 6 шаге электронное устройство подписывает документ, подписывает журнал. Электронные подписи платежного поручения и журнала операции отправляются на сервер на проверку. Сервер своей памяти журнал операций как доказательную базу для возможных расследований.

Таким образом, в устройствах класса TrustScreen используется принципа SWYX (Sign What You eXecuted, Подписываю все, что выполняю). Использование устройств данного класса обладает следующими преимуществами:

- формирование доказательной базы для расследований. Операции подписываются закрытым неизвлекаемым ключом токена с экраном, что практически делает не возможным подделку ЭП;

- защищает клиента, работающего в не доверенной среде, от самых распространенных атак;

- сокращение затрат и времени на подтверждение подозрительных платежей через Call-центры. Эти операции производятся через устройства класса TrustScreen[71].

В целом, у бизнеса появляется возможность строить многоуровневую систему работы с ДБО, используя следующие средства:

- логин и пароль, СКЗИ. Используется для ограниченного количества операций с заданием суточного лимита;

- USB-токен. Доступны практически все операции, но есть ограничения по суточному лимиту или для подозрительных операций требуется подтверждение через телефон;

- устройства класса TrustScreen. Доступны все операции.

Примерами устройств данного класса являются «Антифрод-терминал» фирмы «Алладин», Рутокен-Pinpad фирмы «Актив».

**4 Электронная подпись и инфраструктура открытых ключей**

**4.1 Электронная подпись**

Последние годы характеризуются активным развитием систем электронного документооборота, облегчающие процесс создания, управления доступом и распространения электронных документов, а также обеспечивающие контроль над потоками документов в организации[73]. При этом обмен данными осуществляется либо через компьютерную сеть, либо сеть Интернет. Кроме того все больше организаций сдают отчетность в электронном виде, участвуют в электронных торгах. Многие государственные организации предоставляют услуги в электронном виде. Во всех данных системах требуются методы и средства, обеспечивающие защиту от модификации и подделки, определение авторства документа. Для решения данных задач используется электронная подпись (ЭП).

В федеральном законе от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" дается следующее определение ЭП: информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В данном документе определены основные виды электронной подписи:

-простая ЭП. В общем случае, подтверждением формирования простой электронной подписи является использование паролей, кодов. Например, вход в личный кабинет, используя логин и пароль;

- усиленная неквалифицированная подпись;

- усиленная квалифицированная подпись.

Усиленная подпись получается в результате криптографического преобразования с использованием ключа электронной подписи, и позволяет определить авторство документа и его целостность. Отличие квалифицированной подписи от неквалифицированной заключается в том, что в первом случае используется цифровой сертификат, полученный от аккредитованного удостоверяющего центра. При этом используются только сертифицированные средства криптографического преобразования.

Простая и усиленная неквалифицированная подпись электронная подпись соответствует бумажному носителю с собственноручной подписью, а усиленная – собственноручной подписи и печати.

На рисунке 4.1 представлена схема формирования и проверки электронной подписи.



Рисунок 4.1 –Схема формирования и проверки электронной подписи

Электронная подпись основана на применении следующих криптографических преобразований:

- ассиметричного шифрования с закрытыми и открытыми ключами;

- функции хеширования.

При формировании подписи контрагента ***A*** при помощи средств криптографического преобразования рассчитывается значение хеш-функции ***X***. Далее значение X зашифровывается ассиметричным алгоритмом шифрования закрытым ключом цифрового сертификата владельца ***Kpriv***. Результат шифрования и является электронной подписью ***ES***, который передается вместе с документом и сертификатом с открытого ключа. Таким образом, электронная подпись на уровне реализации представляет собой зашифрованное хеш-значение документа.

Контрагенту ***B*** известны алгоритмы шифрования и хеширования. Таким образом, на основании полученного документа рассчитывается текущее значение хеш-функции ***XD***. При помощи открытого ключа сертификата владельца документа расшифровывается ***XE*** , сформированныйконтрагентом ***A***. Совпадение значение рассчитанного и полученного значений хеш-функции свидетельствует о целостности документа. Несмотря на то, что злоумышленнику также известен алгоритм хеширования, он не может сформировать новую электронную подпись модифицированному документу, так как не знает закрытый ключ ***Kpriv***. Авторство владельца документа подтверждается тем, что расшифровать ЭП можно только открытым ключом контрагента A. Открытый ключ распространяется в виде цифрового сертификата, который позволяет проверить соответствие открытого ключа определенному пользователю.

Стойкость системы формирования/проверки электронной подписи зависит от выбранных алгоритмов шифрования и хеширования, надежности хранения закрытого ключа, от уровня защиты удостоверяющего центра, выдающего цифровые сертификаты. В связи с этим, в государственных информационных системах использующих электронные формы сдачи отчетности, предоставления электронных услуг регламентируется использования только сертифицированных средств для формирования усиленной квалифицированной электронной подписи. Примерами подобных средств являются ПО «КриптоАрм», «Криптэк», библиотека «КриптоПро CSP». При этом цифровой сертификат владельца должен быть получен только из аккредитованных центров.

**4.2 Цифровой сертификат стандарта X.509**

В системах формирования/проверки усиленной электронной подписи используется цифровой сертификат, позволяющий удостовериться, что представленный в нем открытый ключ действительно принадлежит пользователю с заданными реквизитами. Данный механизм позволяет безопасно распространять открытый ключ, защищая от атаки злоумышленника, когда он представляет свой открытый ключ как ключ легального пользователя. Можно привести аналогию с паспортом: при наличии фотографии, подписи и печати ФМС, наличия водяных подтверждаются, что представленные данные соответствуют конкретному человеку.

Наиболее распространенным форматом цифрового сертификата является стандарт X.509. Сертификат выполняет следующую функцию: служит контейнером для открытого ключа, который может быть использован для проверки или валидации конечного субъекта, такого как веб-сайт, пользователь. Цифровой сертификат содержит информацию четырех типов: идентификационные данные субъекта, открытый ключ субъекта, данные удостоверяющего центра (УЦ), подписавшего его, и электронная подпись, сформированная УЦ. Удостоверяющий центр это субъект, который имеет право подписывать сертификаты[74]. На рисунке 4.2 представлена схема формирования ЭП цифрового сертификата.



Рисунок 4.2- Схема формирования электронной подписи цифрового сертификата

Удостоверяющий центр формирует электронную подпись при помощи своего закрытого ключа над следующими данными: данные субъекта, открытый ключ субъекта, данные издателя сертификата. Пользователь передает свой сертификат всем остальным участникам электронного взаимодействия. Остальные субъекты имеют возможность проверить сертификат, и убедится, что открытый ключ действительно принадлежит определенному пользователю. Схема проверки сертификата представлена на рисунке 4.3.



Рисунок 4.3- Схема проверки цифрового сертификата

В проверяющей системе необходимо наличие сертификата удостоверяющего центра, который часто подписан самим УЦ. Информация об используемых алгоритмах шифровании и хеширования представлены в самом сертификате. При помощи открытого ключа УЦ расшифровывается ЭП проверяемого сертификата. Одновременно рассчитывается текущее значение хеш-функции ***XD***. Одинаковые значения хеш-функций свидетельствует о корректности сертификата.

Кроме того существуют дополнения сертификата, позволяющие включать в него информацию, которая отсутствует в основном содержании, определять валидность сертификата и наличие у владельца сертификата прав доступа к той или иной системе[75]. Данные дополнения делятся на два класса:

- ограничивающие область применения ЦС;

-информационные, содержащие дополнительную информацию для прикладных программ организации.

На рисунках 4.4 и 4.5 представлено окна отображения основных и дополнительных полей сертификата средствами ОС Windows.

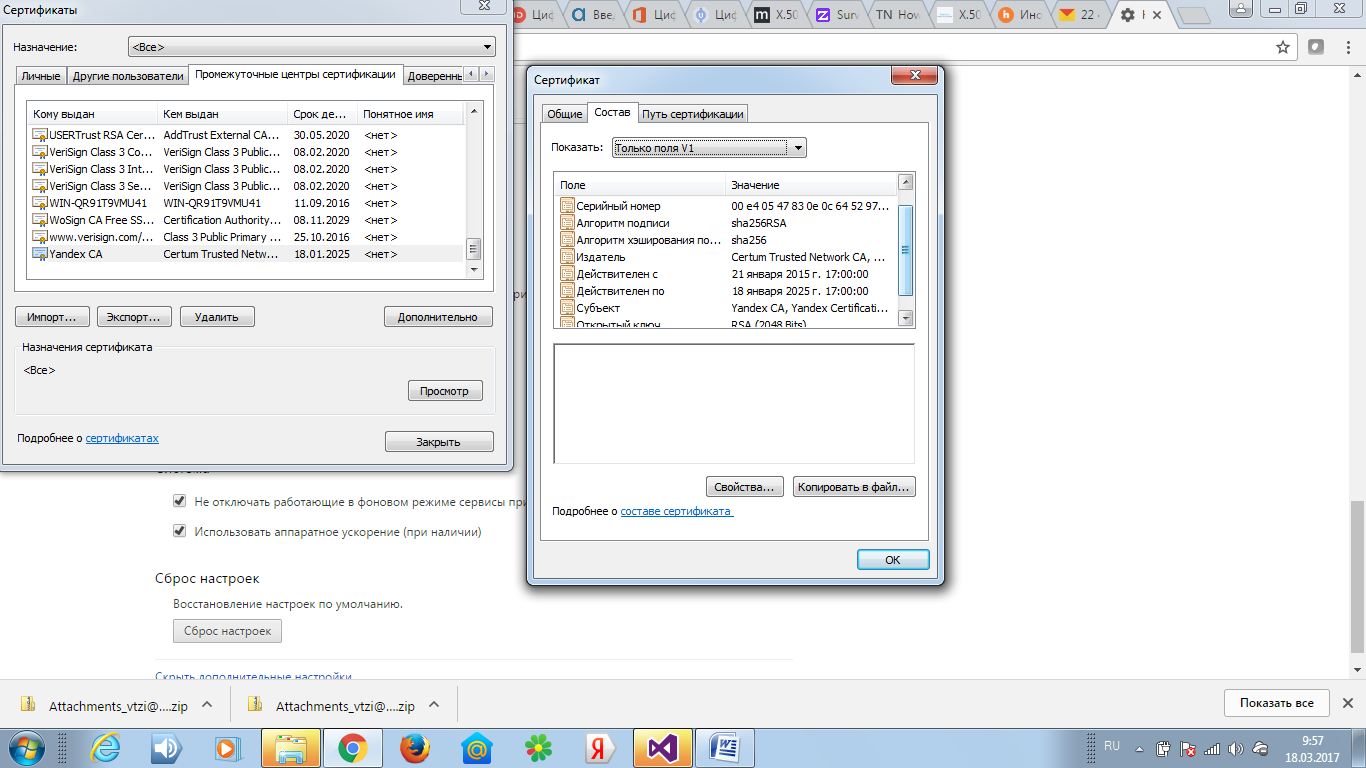
ё

Рисунок 4.4 – Основные поля сертификата

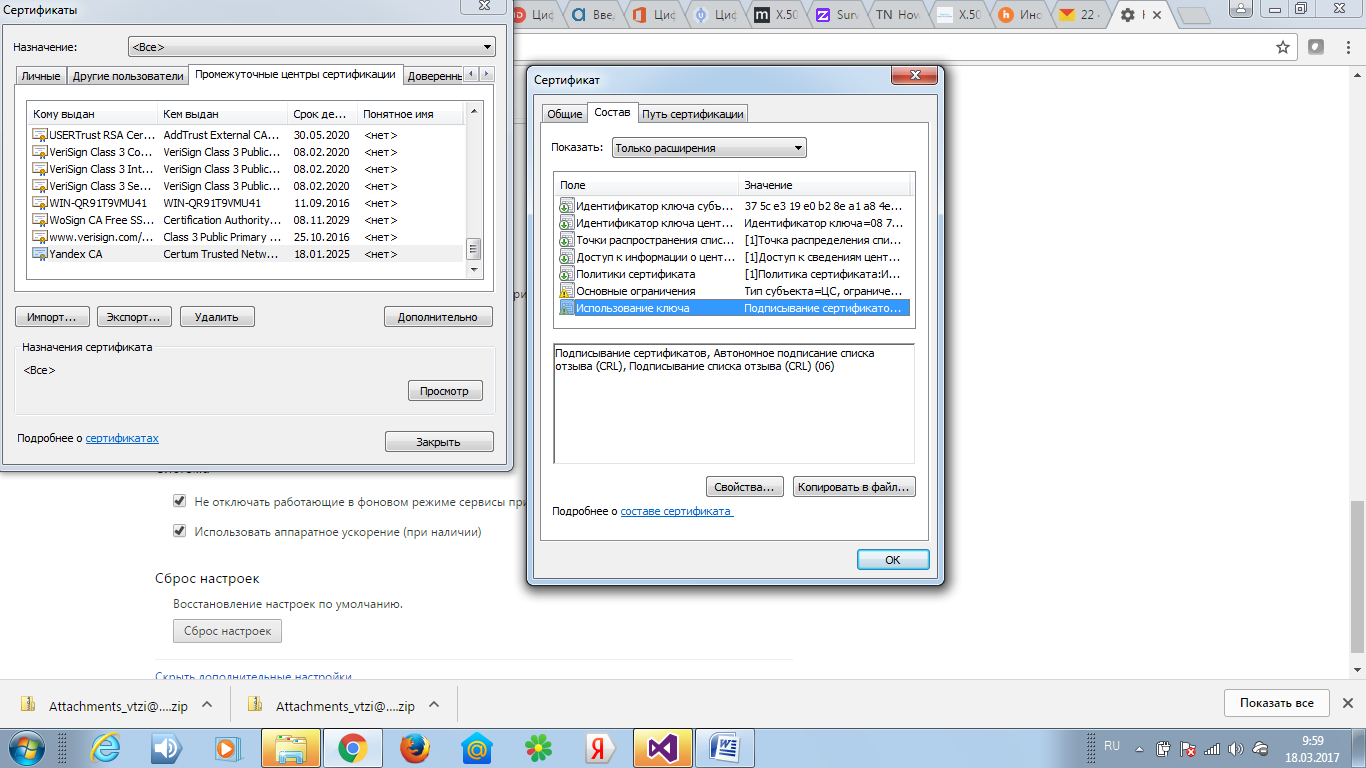


Рисунок 4.5 – Дополнительные поля сертификата

Прикладные программы, кроме проверки корректности ЭП сертификата, учитывают период действия ЦС, назначение ключа.

Также необходимо отметить, что система использования цифровых сертификатов основывается на доверии всех участников к третьей сторон - удостоверяющему центру. При этом у всех участников в системе должен присутствовать сертификат УЦ с открытым ключом, полученный из доверенного источника. Использование цифровых сертификатов является важным элементом систем защищенного электронного документооборота.

**4.3 Усовершенствованная электронная подпись**

Большинство государственных организаций принимают электронные документы, подписанные только квалифицированной ЭП [17].

Квалифицированная ЭП обладает рядом уязвимостей:

– нет доказательства момента подписи;

– трудность доказывания статуса сертификата открытого ключа подписи на момент подписи (или действителен, или аннулирован, или приостановлен)[15].

Для исправления данных недостатков предложен европейский стандарт CMS Advanced Electronic Signatures (CAdES) [28].На рисунке 4.5 представлена структура усовершенствованной электронной подписи.

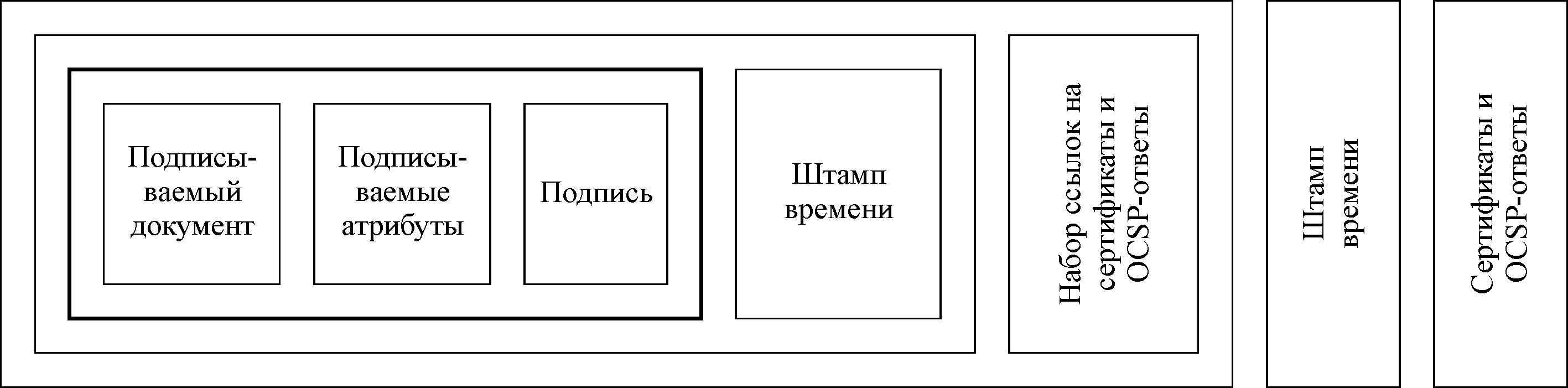


Рисунок 4.6 – Формат усовершенствованной электронной цифровой

подписи [24, с. 4]

При подписании ЭП документа выполняются следующие действия:

* формирование ЭП электронного документа;
* получение штампа времени от TSP-сервера на значение хеш-функции документа. Сервер шифрует штамп времени закрытым ключом;
* осуществляется сбор доказательства действительности сертификата подписывающей стороны у OCSP-сервера;
* далее получается штамп времени о том, что во время создания ЭП доказательства действительности сертификата были корректны.

Для формирования усовершенствованной электронной подписи необходимо наличие двух доверенных серверов: TSP( Time Stamp Protokol) и OSCP (On-line Certificate Status Protocol). TSP –сервер содержит точный источник времени и предназначен для формирования «штампа времени» на данные от клиентов по запросу. OSCP-сервер используется для получения текущего статуса сертификата[76].

Структурная схема системы формирования усовершенствованной электронной подписи представлена на рисунке 4.6.



Рисунок 4.6 –Схема формирования усовершенствованной подписи

На первом шаге программное средства пользователя формирует электронную подпись ***XD*** над данными ***D***.С целью подтверждении момент времени формирования подписи осуществляется запрос к TSP-серверу с передачей ему ***XD***. Сервер формирует штамп времени ***TD***, состоящий из следующих частей:

- электронная подпись документа на сертификате пользователя;

- отметка времени, сформированная сервером;

- электронная подпись над двумя предыдущими полями, сформированная на сертификате TSP-сервера.

На следующем шаге пользователь формирует запрос к OCSP-серверу ***S***1, чтобы получить доказательства корректности статуса. На электронную подпись документа ***XD***, хеш-коды доказательств подлинности ***S***2 ставится штамп времени ***TS***.

Таким образом, применение усовершенствованной электронной подписи обладает следующими преимуществами:

- доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент;

- отсутствие необходимости сетевых обращений при проверке подписи;

- архивное хранение электронных документов[77].

**4.4 Инфраструктура открытых ключей**

Для обеспечения информационной безопасности компьютерных систем, в частности, конфиденциальности и целостности данных, основными методами являются шифрование, применение электронной подписи, методов аутентификация и авторизация. Эффективность данных методов для обеспечения требуемого уровня защищенности определяется возможностью безопасного распределения ключей, особенно в распределенных системах. Решением данной задачи является использование ассиметричных алгоритмов шифрования с использованием открытых и закрытых ключей, например, Диффи-Хэллмана или RSA[78]. Использование ассиметричных алгоритмов требует проверки соответствия идентификационных данных пользователя и открытого ключа конечного пользователя.

Таким образом, распространение ключей алгоритмов шифрования может выполняться тремя основными способами:

- прямым обменом между сторонами при помощи симметричного шифрования;

- посредством симметричного шифрования и доверенной третьей стороны;

- при помощи управления открытыми ключами доверенной третьей стороной[78].

Первый способ предполагает обмен симметричными ключами при помощи безопасных каналов передачи данных, например, из рук в руки или фельдъегерской службой. Данный подход может быть применен только для информационного взаимодействия, предполагающих не более 5 участников.

Второй вариант предполагает наличие доверенного узла, который формирует сеансовый ключ для взаимодействия участников информационного взаимодействия. Примером данного способа является реализация протокола Kerberos. Несмотря на хорошую масштабируемость данного подхода существует основные недостатки:

- невозможность использования сформированного ключа для аутентификации;

- невозможно реализовать неотказуемость от определенного действия, так как ключ шифрования известен нескольким участникам.

Наиболее популярным решением для распространения ключей алгоритмов шифрования является инфраструктура открытых ключей (PKI),позволяющая обеспечить требования информационной безопасности по обеспечению конфиденциальности, целостности, аутентичности, не отрицания авторства.

Инфраструктура открытых ключей представляет собой совокупность программного обеспечения, алгоритмов шифрования и сервисов, позволяющих обеспечить информационную безопасность электронного информационного взаимодействия[79], основанную на цифровых сертификатах. Основными элементами PKI являются:

-удостоверяющий центр;

- регистрационный центр;

- репозиторий сертификатов;

- архив сертификатов;

- конечные пользователи [80].

На рисунке 4.7 представлена схема взаимодействия основных элементов инфраструктуры открытых ключей.



Рисунок 4.7 – Структурная схема инфраструктуры открытых ключей

Удостоверяющий центр является основным элементом PKI и выполняет следующие функции:

- создает сертификаты открытых ключей конечных субъектов и подчи ненных УЦ;

- формирует списки аннулированных сертификатов.

Пользователь обычно генерирует ключевую пару (открытый и закрытый клич)и отправляет запрос ***D*** с своими идентификационными данными регистрационному центру (РЦ) на получение сертификата. РЦ регистрирует пользователя и проверяет корректность представленных в запросе данных. При успешной проверке запроса пользователя регистрационный центр формирует запрос к УЦ на получение сертификата ***DR***. В ответ удостоверяющий центр формирует сертификат на основе открытого ключа пользователя и его идентификационных данных и подписывает своим закрытым ключом. Сформированный сертификат передается пользователю, кроме того публикуется в репозитарий. Также удостоверяющий центр периодически передает в репозитарий списки отозванных сертификатов. Архив сертификатов используется для долговременного хранения всех изданных сертификатов. В различных реализациях схема PKI может изменяться.

Пользователь может использовать сертификаты для различных целей: аутентификации, шифрования данных, формирования электронной подписи. Уровень информационной безопасности информационных систем, использующих инфраструктуру открытых ключей, во многом зависит от степени защищенности удостоверяющего центра. Компрометация закрытого ключа УЦ приведет приведёт к потере доверия к сертификатам конечных пользователей.

Для различных организаций используют различные архитектуры PKI, отличающиеся количеством удостоверяющих центров и структурой связей. Для небольших организаций достаточно одного удостоверяющего центра. Крупные организации, особенно имеющие распределенную архитектуру, для обеспечения требуемого уровня безопасности могут использовать более сложные архитектуры инфраструктуры открытых ключей, такие как иерархические и сетевые. На рисунке 4.8 представлена иерархическая структура PKI.



Рисунок 4.8 – Иерархическая архитектура инфраструктуры открытых ключей

Удостоверяющий центр издает сертификат своим нижестоящим подчиненным УЦ и конечным пользователям. Таким образом, формируется путь сертификации от головного УЦ до нижестоящих удостоверяющих центров. Данная архитектура быстро реагирует на компрометацию сертификата УЦ – вышестоящий центр просто аннулирует его сертификат. Это приводит к недействительности и сертификатов субъектов скомпрометированного УЦ. Компрометация головного УЦ приводит к тяжелым последствиям и остановке работы системы, так как все выданные сертификаты в рамках данной PKI являются недействительными. Преимущество иерархической архитектуры по сравнению с одиночным УЦ заключается в том, что в случае компрометации головного центра требуется выпустить существенно меньшее количество новых сертификатов. Кроме того головной УЦ может оперировать автономно, значительно сокращая вероятность компрометации своего ключа[80].

**4.5 Лабораторная работа. Инфраструктура открытых ключей Windows Server 2008**

**Цель работы:** получить навыки работы развертывания PKI.

4.5.1 Теоретическая часть

Серверные операционные системы Windows позволяют реализовать инфраструктуру открытых ключей для решения различных задач. Типовыми сценариями использования PKI являются:

- шифрование диска и файлов (сертификаты используются для защиты симметричного крипто ключа symmetric crypto key);

- двухфакторная аутентификация ;

- IPSec- протокол;

- цифровая подпись;

- аутентификация RADIUS и 802.1x authentication;

- NAP (Network Access Control);

- SSL/TLS для защиты HTTP трафика[81].

В Windows Server 2008 R2 добавлены такая возможность, как веб-служба развертывания сертификатов, позволяющая клиентам получать сертификаты по http-протоколу. В данной ОС выделены следующие основные роли центров сертификации: головной центр сертификации (ЦС) предприятия, подчиненный центр сертификации предприятия, самостоятельный головной центр сертификации, самостоятельный подчиненный центр сертификации. Отличие ЦС предприятия от самостоятельного заключается в том, что первый связан с доменом.

Перед развертыванием PKI необходимо определить её структуру. Выделяют три основные архитектуры: одноуровневая, двухуровневая и многоуровневая. Одноуровневая PKI предполагает применение для небольшой компании, оперирующей небольшим количество сертификатов. Один и тот же центр сертификации является корневым ЦС и выдающим ЦС. Данная структура характеризуется низким уровнем безопасности, так как компрометация ЦС приводит к потере доверия к выданным сертификатам. К достоинству одноуровневой PKI может относится только простота развертывания и администрирования[82].

Более безопасным является использование двухуровневой инфраструктуры открытых ключей. В данной схеме корневой центр сертификации работает автономно и даже лучше, если он не подключении к сети. Это позволит снизить риск компрометации его сертификата. Выдающие ЦС на втором уровне могут быть распределены либо географически, либо по назначению выдаваемых сертификатов. Второй способ используется для ограничения выдачи подчиненным ЦС сертификатов, которые могут использоваться для непредусмотренных целей.

Многоуровневой системе выделяются дополнительные уровни. Это позволяет при компрометации сертификатов ЦС нижних уровней осуществить отзыв сертификата не главного центра, а более низкого. Следуя этой парадигме, безопасность возрастает при добавлении уровня, а гибкость и масштабируемость — благодаря расширению вариантов структуры. С другой стороны, это также влияет на управляемость, так как в иерархии появляется большее число управляемых ЦС и затраты растут[82].

4.5.2 Постановка задачи

В работе предполагается, что есть контроллер домена и рабочая станция, под управлением ОС Windows 7. Необходимо выполнить следующие задачи:

- контроллеру домена добавить роли центра сертификации предприятия и службу веб-службу развертывания сертификатов;

- создать учетную запись администратора безопасности, который имеет право формировать запросы на получение сертификата для других пользователей;

- настроить права доступа к шаблонам сертификатов;

-создать групповую политику для распространения сертификата ЦС на все компьютеры домена;

-создать подразделение для пользователей с смарт-картой и создать для неё групповую политику, позволяющую запретить вход в систему без смарт-карты;

- получить через веб-интерфейс сертификат администратора безопасности на клиентской машине;

- получить администратором безопасности для другого пользователя сертификат и сохранить его на смарт-карту.

4.5.3 Порядок выполнения работы

1. Выберите в Windows Server 2008 пункт меню «Пуск|Администрирование|Диспетчер сервера».

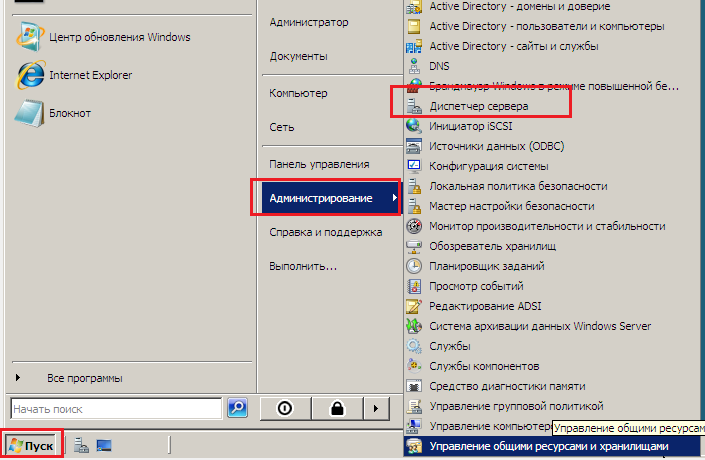


Рисунок 4.9 –Окно выбора пункта меню «Диспетчер сервера»

1. В окне «Диспетчера сервера» выберите раздел «Роли» и справа нажмите на ссылку «Добавить роли».

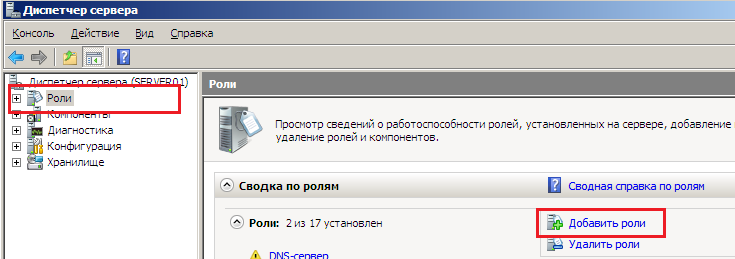


Рисунок 4.20 –Окно «Диспетчер сервера»

1. В появившемся окне нажмите кнопку «Далее».
2. В окне выбора роле сервера выставьте флажок «Службы сертификации Active Directory».



Рисунок 4.11 –Окно выбора ролей сервера

1. Нажмите кнопку «Далее». Прочитайте предупреждение «Мастера добавления ролей» о невозможности изменения имени и домена данного компьютера после установки центра сертификации. Нажмите кнопку «Далее».
2. В появившемся окне выбора службы ролей для установки службы сертификации выставьте флажок «Служба подачи заявок через Интернет». В появившемся дополнительном окне с сообщением о необходимости установки дополнительных служб нажмите на кнопку «Добавить требуемые службы роли».

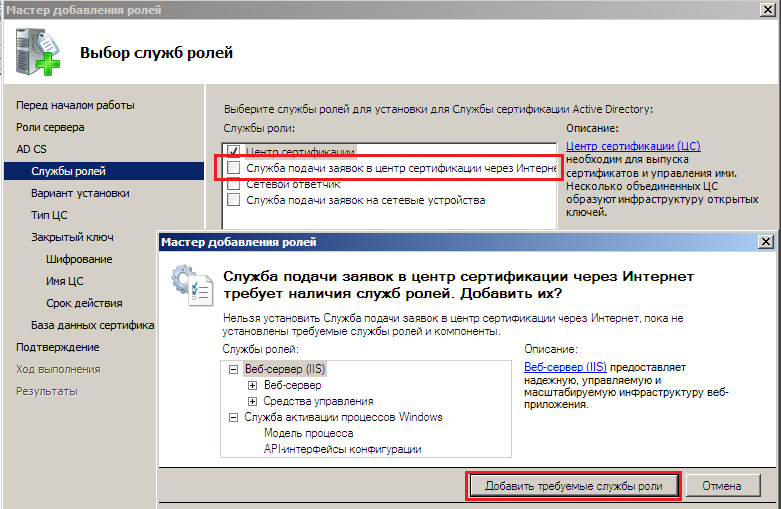


Рисунок 4.12 –Окно выбора служб сервера

1. Нажмите кнопку «Далее». Выберите вариант установки центра сертификации «Предприятие» и нажмите кнопку «Далее».
2. Выберите тип центра сертификации «Корневой» и нажмите кнопку «Далее».
3. Укажите, выбрав пункт «Создать новый закрытый ключ», что нужно создать новый ключ.
4. В окне выбора поставщика служб шифрования оставьте значения настроек по умолчанию (результат должен быть как на рисунке ниже).

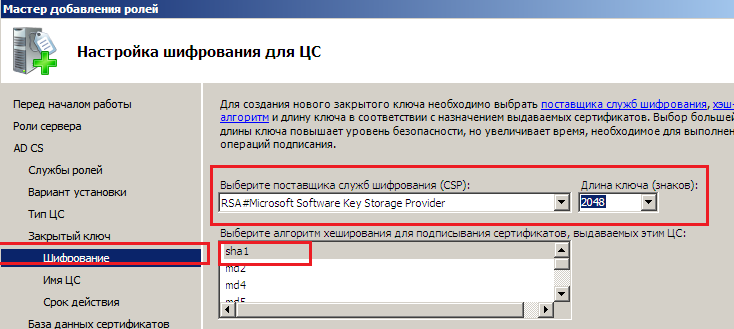


Рисунок 4.13 –Окно выбора параметров шифрования

1. Нажмите кнопку «Далее».
2. Просмотрите общее имя центра сертификации и нажмите «Далее».
3. Срок действия сертификата измените на 20 лет и нажмите кнопку «Далее».
4. Нажимайте кнопку «Далее», оставляя в в окнах настроек значения по умолчанию, пока не перейдете к пункту «Подтверждение».
5. Нажмите кнопку «Установить». Подождите, пока не закончится процесс установки выбранных служб.
6. Убедитесь, что выбранные службы установлены и нажмите кнопку «Закрыть».

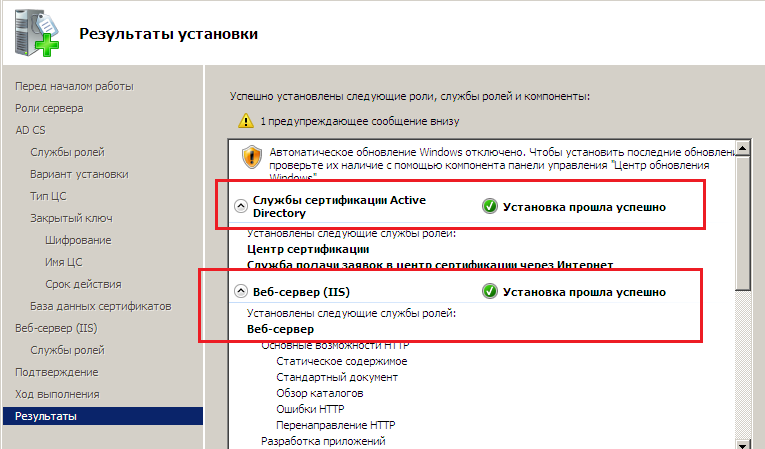


Рисунок 4.13 –Результаты установки службы сертификации

1. Закройте программу «Диспетчер сервера».
2. Выберите пункт меню «Пуск| Администрирование| центр сертификации».
3. В открывшемся окне выберите раздел «Выданные сертификаты» и убедитесь, что под кодом 2 выдан сертификат контроллеру домена.

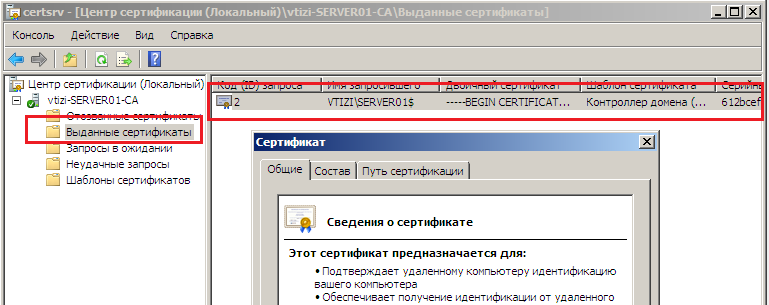


Рисунок 4.14 –Окно просмотра выданных сертификатов

1. Закройте окно «Центр сертификации».
2. Выберите пункт меню «Пуск | Администрирование | Active Directory – пользователи и компьютеры». Выделите домен «vtizi.net и создайте подразделение «SecurityAdmins».
3. В подразделении «SecurityAdmins» создайте глобальную группу безопасности «g\_SecurityAdmins».

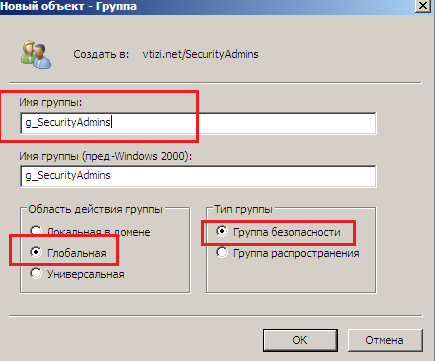


Рисунок 4.15 –Параметры глобальной группы безопасности

1. Также в этом подразделении создайте локальную группу «d\_Enrollment\_agents».

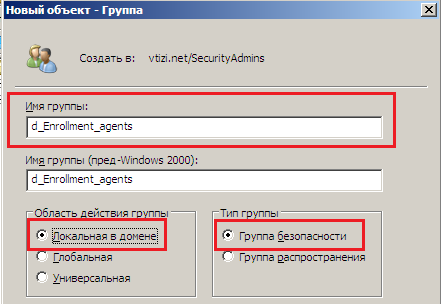


Рисунок 4.16 –Параметры группы безопасности

1. Выделите группу «g\_SecurityAdmins» и нажатием правой кнопки мыши, вызовите контекстное меню, в котором выберете пункт «Свойства». Перейдите на вкладку «Член групп» и нажмите на кнопку «Добавить».

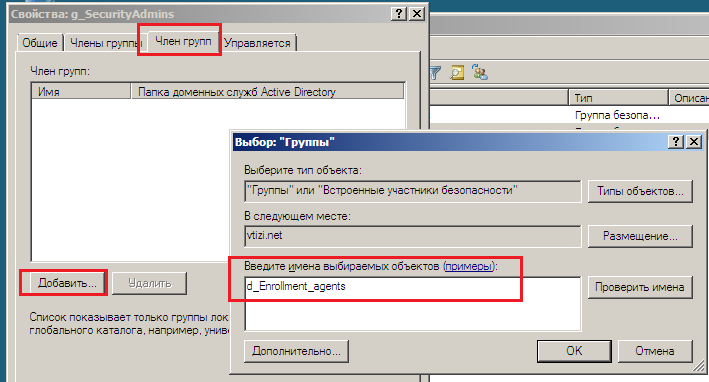


Рисунок 4.17 –Параметры группы безопасноти

1. В появившемся окне введите имя группы «d\_Enrollment\_agents» и нажмите на кнопку «OK». В окне свойств группы нажмите на кнопки «Применить» и «OK».
2. В подразделении «SecurityAdmins» создайте пользователя «enrollment\_agent».

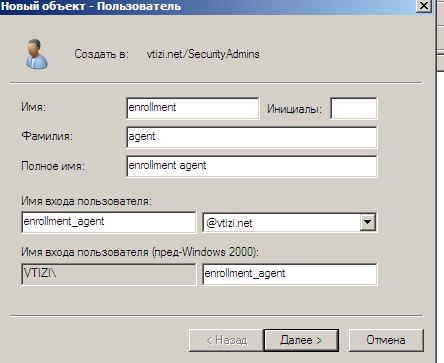


Рисунок 4.17 –Параметры учетной записи

1. На следующем окне введите пароль пользователя, уберите флажок «Требовать смену пароля при следующем входе в систему». Нажмите на кнопку «Далее» и в следующем окне «Готово».
2. Добавьте пользователя «enrollment\_agent» в группу «g\_SecurityAdmins»

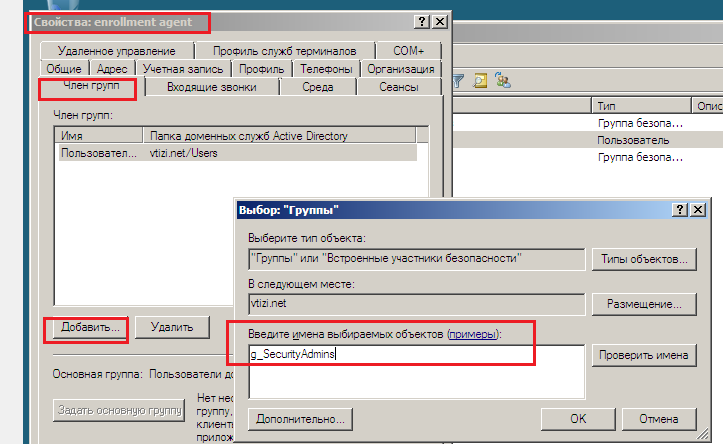


Рисунок 4.18 –Окно выбора группы для учетной записи

1. Выберите пункт меню «Пуск| Администрирование| Центр сертификации». В появившемся окне выделите раздел «Шаблоны сертификатов». Вызовите контекстное меню и выберите пункт «Управление».

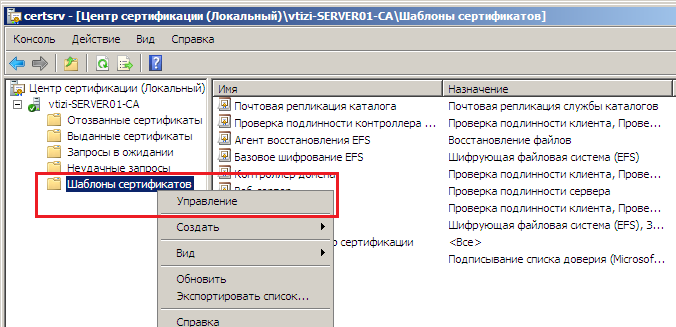


Рисунок 4.19 –Окно выбора шаблона сертификата

1. В появившемся окне «Консоль шаблонов сертификатов» выберите шаблон «Агент подачи заявок».
2. Дважды щелкните на этом шаблоне и перейдите на вкладку «Безопасность». Нажмите на кнопку «Добавить». В появившемся окне введите имя группы «d\_Enrollment\_agents». Выставьте данной группе права «Чтение» и «Заявка».

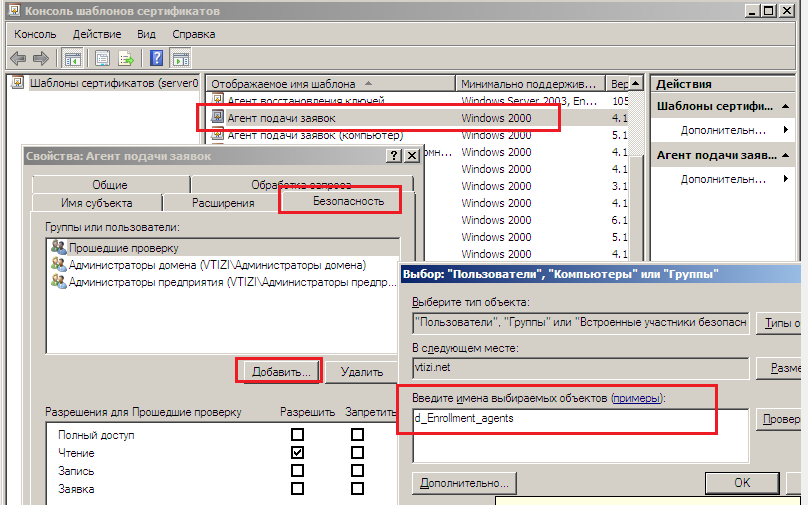


Рисунок 4.20 –Окно настроек шаблона сертификата

1. То же самое делаем для шаблона «Вход со смарт-картой».

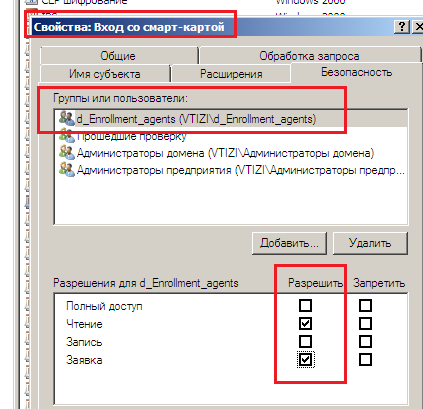


Рисунок 4.21 –Окно настроек шаблона сертификата «Вход с смарт-картой»

1. Перейдите в окно центр сертификации, выберите раздел «Шаблоны сертификатов». В контекстном меню выберите операцию «Создать| Выдаваемый шаблон сертификата».

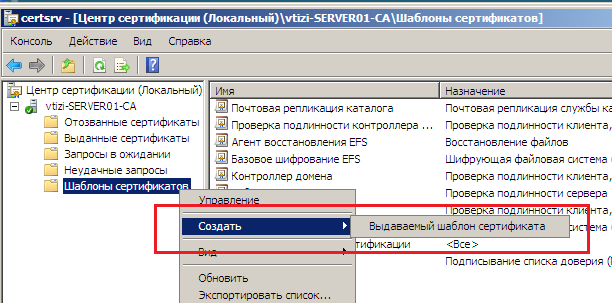


Рисунок 4.22 –Окно создания шаблона сертификата

1. В окне «Включение шаблонов сертификатов» выберите «Агент подачи заявок» и «Вход со смарт-картой».

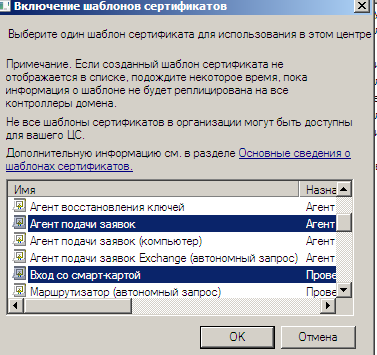


Рисунок 4.23 –Окно «Включение шаблонов сертификатов»

1. Нажмите на кнопку «OK». Закройте все окна.
2. Выберите пункт меню «Пуск| Администрирование| Центр сертификации| Управление групповой политикой». Выберите в окне групповую политику «Default Domain Policy». В контекстном меню выберите пункт «Изменить».

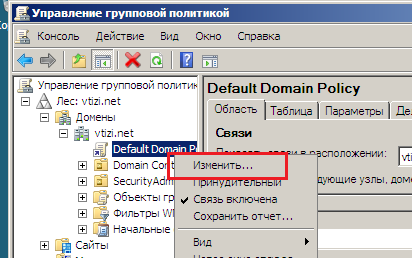


Рисунок 4.24 –Окно «Управление групповой политикой»

1. Выберите раздел «Конфигурация компьютера/Политики/ Конфигурация Windows/ Параметры безопасности/ Политики открытого ключа/ Доверенные корневые центры сертификации». Вызовите контекстное меню и выберите пункт «Импорт».



Рисунок 4.25 –Окно изменения политики открытого ключа

1. В мастере импорта сертификатов нажмите на кнопку «Обзор» и выберите сертификат из папки «C:\Windows\System32\certsrv\CertEnroll». Нажмите кнопки «Далее» и «Готово». Закройте окно редактирования групповой политики.

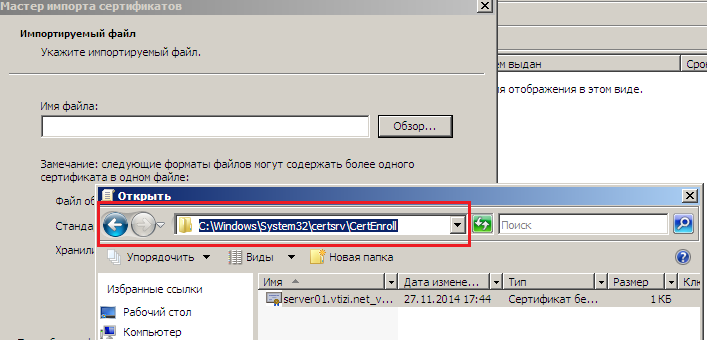


Рисунок 4.26 –Окно выбора сертификата

1. В окне «Управление групповой политикой» создайте подразделение «Пользователи со смарт-картой» в домене vtizi.net.

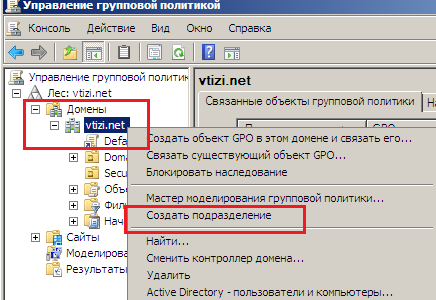


Рисунок 4.27 –Окно создания подразделения

1. Выделите подразделение «Пользователи со смарт-картой» и в контекстном меню выберите «Создать объект GPO в этом домене и связать его». Введите имя групповой политики «SmartCard GPO» и нажмите кнопку «OK».
2. В контекстном меню групповой политики «SmartCard GPO» выберите пункт «Изменить». Выберите раздел «Конфигурация компьютера/Политики/ Конфигурация Windows/ Параметры безопасности/ Локальные политики / Параметры безопасности».
3. Включите политику «Интерактивный вход в систему: требовать смарт-карту».

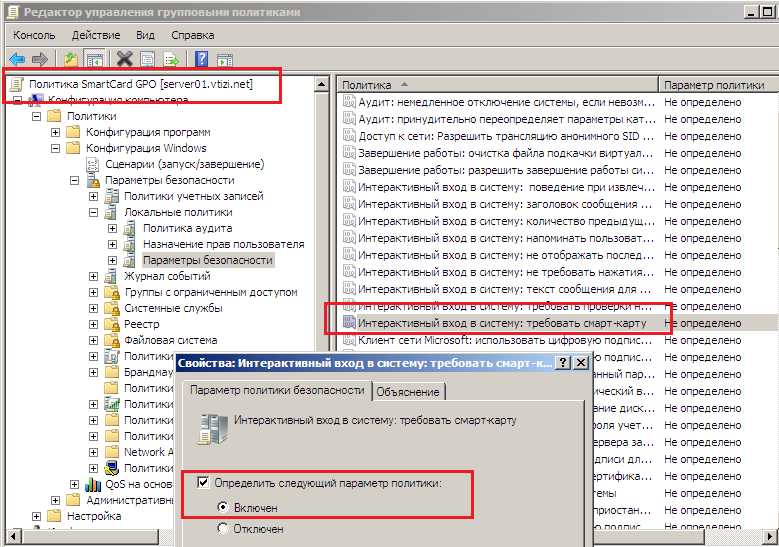


Рисунок 4.28 –Окно изменения групповой политики

1. Определите политику «Интерактивный вход в систему: поведение при извлечении смарт-карты» в значение «Принудительный выход из системы».

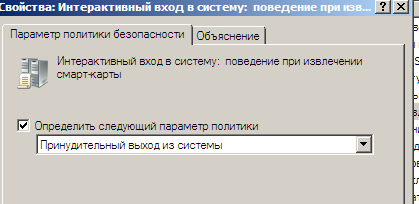


Рисунок 4.29 –Окно редактирования политики

1. Выберите раздел в редакторе групповой политики «Конфигурация компьютера/Политики/ Конфигурация Windows/ Параметры безопасности/ Системные службы». Выберите политику «Политику удаления смарт-карт» и укажите режим запуска «Автоматически».

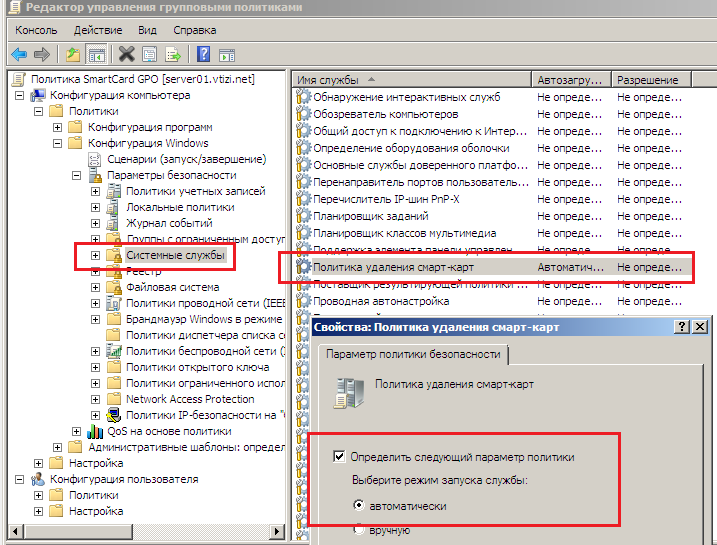


Рисунок 4.30 –Окно редактирования политики

1. Закройте все окна. Запустите приложение «Командная строка» и наберите команду «gpupdate» для обновления групповых политик.
2. Зайдите на клиентский компьютер под учетной записью «enrollment\_agent».
3. Запустите браузер «Internet Explorer» и наберите адрес «http://server01/certsrv». В свойствах браузерах разрешите выполнение Activex-скриптов.

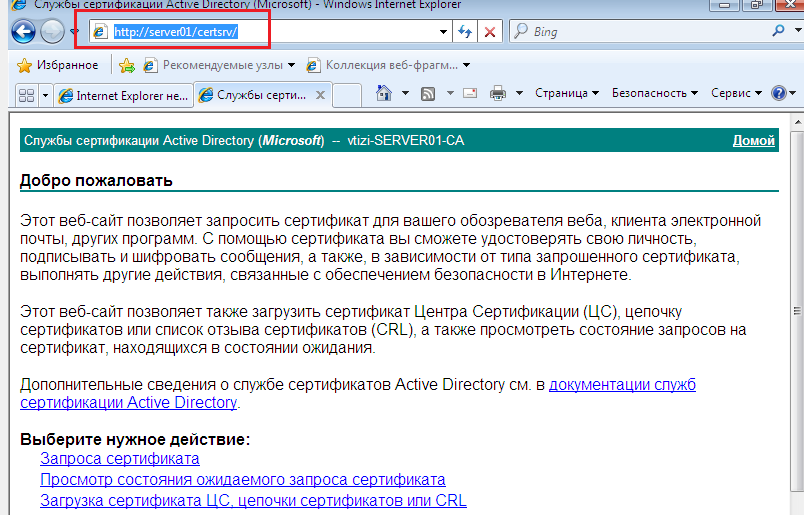


Рисунок 4.31 –Окно сайта службы сертификации

1. Выбираем ссылку «Запрос сертификата». В следующем окне выбираем пункт «расширенный запрос сертификата».
2. Далее выбираем «Создать и выдать запрос к этому ЦС».
3. В следующем окне выберите шаблон сертификата «Агент подачи заявок». Далее нажмите кнопки «Выдать» и «Установить».
4. Закройте браузер. Нажмите кнопку «Пуск» и в поле «Найти программы и файлы» введите строку «certmgr.msc» и запустите данную консоль.
5. В появившемся окне выберите раздел «Личное». В контекстном меню выберите пункт «Зарегистрироваться от имени».

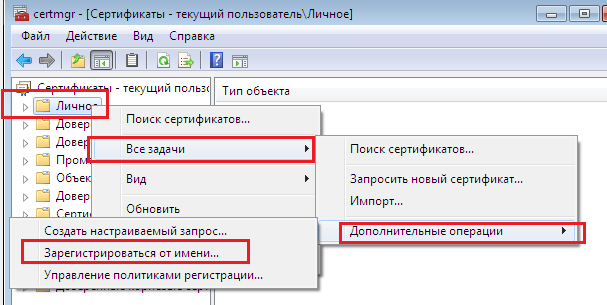


Рисунок 4.32 –Окно консоли «Сертификаты»

1. Нажимайте кнопки «Далее» до тех пор, пока не появится окно выбора сертификата агента регистрации. Выберите сертификат пользователя «enrollment\_agent». Нажмите кнопку «Далее».
2. Выбираем запрос сертификата «Вход со смарт-картой» и нажимаем на ссылку «Подробности».

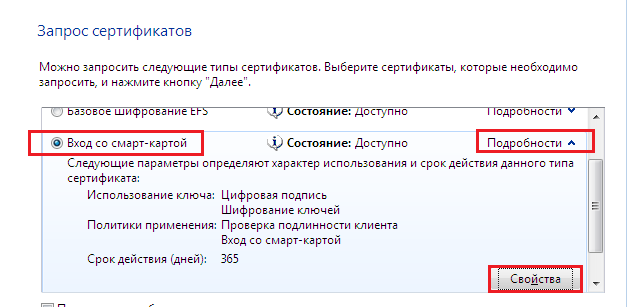


Рисунок 4.33 –Окно настройки параметров сертификата

1. Нажмите на кнопку «Свойства». В разделе «Закрытый ключ» выберите поставщика службы шифрования «Activ ruToken CSP….». Нажмите на кнопку «Далее».

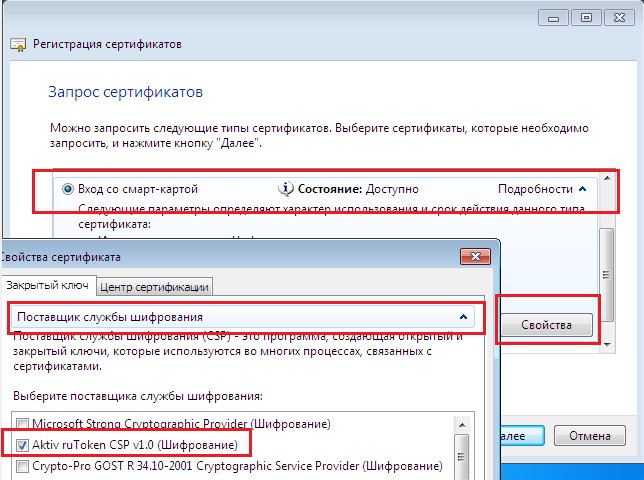


Рисунок 4.34 –Окно «Свойство сертификата»

1. Подтвердите выбор нажатием кнопки «OK». Выберите пользователя из домена.

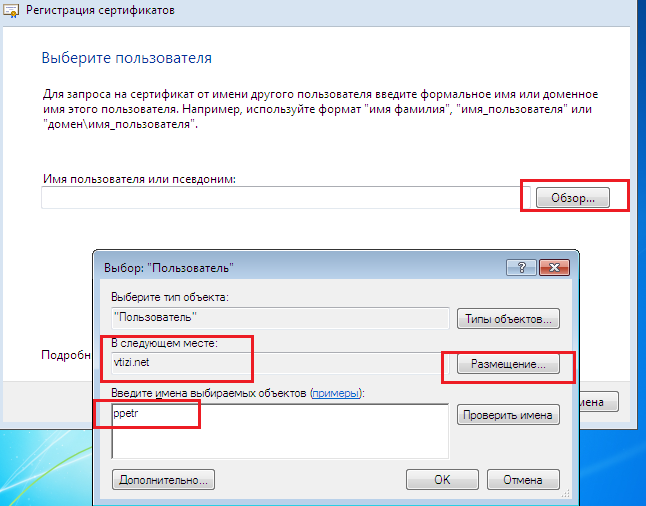


Рисунок 4.35 –Окно выбора пользователя при запросе сертификата

1. Нажмите кнопку и вставьте смарт-карту.

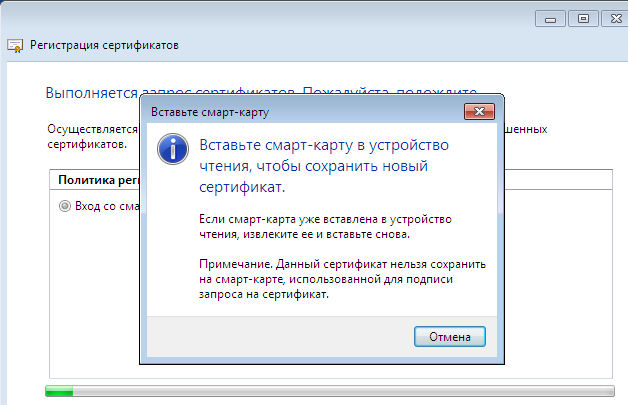


Рисунок 4.36 –Окно подключения смарт-карты

1. На следующем шаге введите PIN-код рутокена. В работе используется PIN-код. Дождитесь окончания процесса установки сертификата и закройте окно.
2. Перейдите на сервер и выберите пункт меню «Пуск| Администрирование | Active Directory – пользователи и компьютеры».
3. Выберите подразделение «Computers», выделите клиентский ПК и в контекстном меню выберите «Переместить».

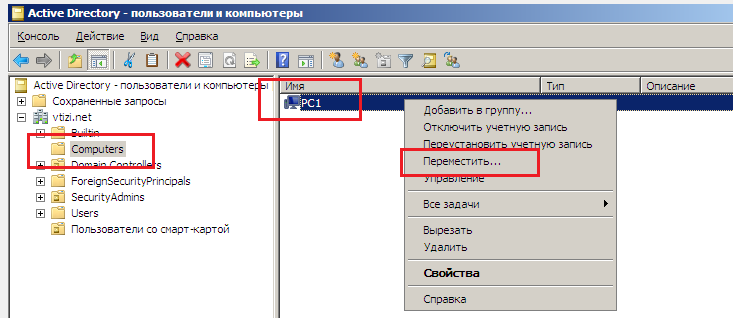


Рисунок 4.37 –Окно подключения смарт-карты

1. Переместите компьютер в подразделение «Пользователи со смарт-картой».

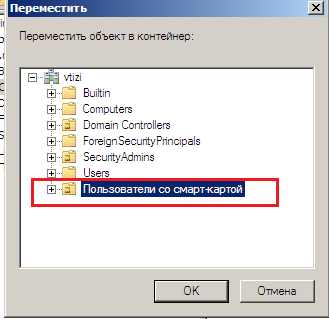


Рисунок 4.38 –Окно перемещения компьютера в подразделение

1. Перейдите на клиентскую машину и перезагрузите компьютер. Попробуйте зайти в систему под учетной записью «enrollment\_agent». Убедитесь, что ОС не пускает без смарт-карты.
2. Нажмите на кнопку сменить пользователя. Выберите пользователя «Петр Петров». Введите пин-код рутокена.

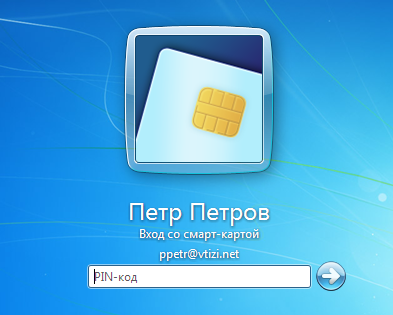


Рисунок 4.39 –Окно входа в систему

1. После входа в систему извлеките рутокен. Убедитесь, что система при извлечении смарт-карты завершит выполнении текущего сеанса пользователя.

**5 Тесты для проверки знаний**

**Тема 1 . Введение. Общая характеристика программно-аппаратных средств защиты информации.**

**1.1** Что понимается под информационной безопасностью:

(Отметьте один правильный вариант ответа.)

1 защита душевного здоровья телезрителей;

**2 защита от нанесения неприемлемого ущерба субъектам информационных отношений;**

3 обеспечение информационной независимости России.

1.2 Что из перечисленного относится к числу основных аспектов информационной безопасности:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

**1 конфиденциальность – защита от несанкционированного доступа к информации;**

2 неотказуемость - невозможность отказаться от совершенных действий;

**3 доступность - возможность за приемлемое время получить требуемую информационную услугу.**

1.3 Сложность обеспечения информационной безопасности является следствием:

(Отметьте один правильный вариант ответа.)

1 наличия многочисленных высококвалифицированных злоумышленников;

**2 комплексного характера данной проблемы, требующей для своего решения привлечения специалистов разного профиля;**

3 развития глобальных сетей.

1.4 Под угрозой безопасности информации в компьютерной системе (КС)

понимают:

(Отметьте один правильный вариант ответа.)

**1 возможность возникновения на каком-либо этапе жизненного цикла КС**

**такого ее состояния, при котором создаются условия для реализации**

**угроз безопасности информации;**

2 событие или действие, которое может вызвать изменение

функционирования КС, связанное с нарушением защищенности

обрабатываемой в ней информации;

3 действие, предпринимаемое нарушителем, которое заключается в

поиске и использовании той или иной уязвимости.

1.5 Основными видами защиты информации являются

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. **правовая защита информации;**
2. **техническая защита информации;**
3. сетевая защита;
4. защита от утечки данных по информационным каналам.

1.6 Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты называется

(Отметьте один правильный вариант ответа.)

1. правовая защита информации;
2. техническая защита информации;
3. криптографическая защита информации;
4. **физическая защита информации.**

1.7 Компьютерная, или автоматизированная система обработки информации включает в свой состав:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. **аппаратные средства;**
2. **данные;**
3. сетевой трафик;
4. **персонал;**
5. средства ограждения и физической изоляции.

1.8 Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является

(Отметьте один правильный вариант ответа.)

1. **обязательное включение в состав технических средств компьютерной системы;**
2. наличие сертификата соответствия ФСТЭК;
3. наличие сертификата соответствия ФСБ;
4. вхождение в состав операционной системы.

1.9 По отношению к компьютерной системе СЗИ являются:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

**1 встроенными;**

2 программными;

**3 внешними;**

4 аппаратными.

1.10 К**омпьютерная система является полностью контролируемой, если можно……**

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. **определить множество выполняемых функций;**

**2 доказать конечность этого множества;**

1. используются аппаратные средства защиты информации;
2. **определить свойства всех функций;**

5 используются аппаратные средства защиты информации.

* 1. К полностью контролируемой операционной системе относится:

(Отметьте один правильный вариант ответа.)

1. **MS DOS;**
2. Windows 8;
3. Linux.
   1. К частично контролируемым компьютерным системам относятся:

(Отметьте один правильный вариант ответа.)

1. **системы, использующие ОС, полностью аттестовать которые не представляется возможным;**
2. системы, использующие полностью аттестованные ОС;
3. системы, использующие ОС семейства Windows;
4. системы, использующие Linux.
   1. Достоинствами аппаратных средств защиты информации являются:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. гибкость и переносимость;
2. **высокая производительность (например, скорость шифрования);**
3. **высокая защищенность от побочных электромагнитных излучений;**
4. простота тиражирования.
   1. Недостатками аппаратных средств защиты являются

(Отметьте один правильный вариант ответа.)

1. прозрачность для пользователя;
2. возможность вмешательства в действия алгоритмов шифрования и получения доступа к ключевой информации;
3. **высокая стоимость;**
4. возможность вмешательства в действия алгоритмов шифрования и получения доступа к ключевой информации.
   1. Достоинства программных средств защиты:

(Отметьте один правильный вариант ответа.)

1. **неограниченные возможности развития путем внесения изменений для учета новых угроз безопасности;**
2. минимальный уровень воздействия на установленное программное обеспечение компьютера;
3. не используются вычислительные ресурсы компьютера;
4. сложность изучения алгоритмов шифрования и получения доступа к ключевой информации.
   1. Достоинствами программно-аппаратных средств защиты компьютерных систем являются:

(Отметьте один правильный вариант ответа.)

**1 обеспечение высокого уровня защищенности и функциональности СЗИ;**

2 гибкость и переносимость;

3 прозрачность для пользователя.

* 1. Функции защиты компьютерных систем, реализующихся на аппаратных средствах

(Отметьте один правильный вариант ответа.)

1. **надежное хранение криптографических ключей вне ОЗУ;**
2. ведение журналов событий;
3. **аппаратный датчик случайных чисел;**
4. реализация криптографических алгоритмов.
   1. Использование внешних сертифицированных средств защиты информации в компьютерных системах определяется:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. **необходимостью соответствовать требованиям законодательства;**
2. **гарантия отсутствия недекларированных функций СЗИ;**
3. удобный интерфейс;
4. низкая стоимость СЗИ.

1.19 Под надежностью системы защиты от несанкционированного копирования понимается:

**1 способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты;**

2 способность к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ;

3 способность разграничения прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;

4 способность использования дополнительных программных или аппаратно-программных средств.

Тема 2. Идентификация пользователей кс-субъектов доступа к данным

2.1 Идентификация объекта – это:

**1 одна из функций подсистемы защиты;**

2 взаимное установление подлинности объектов, связывающихся между

собой по линиям связи;

3 сфера действий пользователя и доступные ему ресурсы КС.

2.2 Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

1 **авторизацией;**

2 аутентификацией;

3 идентификация.

2.3 Авторизация – это:

**1 предоставлением полномочий;**

2 подтверждение подлинности;

3 цифровая подпись.

2.4 Аутентификация – это:

**1 подтверждение подлинности;**

2 предоставлением полномочий;

3 цифровая подпись.

2.5 Для проведения процедур идентификации и аутентификации пользователя необходимо:

1 наличие соответствующего субъекта (модуля) аутентификации;

2 наличие аутентифицирующего объекта, хранящего уникальную информацию;

3 ответы 1) и 2).

2.6 Биометрическая идентификация и аутентификация пользователя это:

**1 идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения;**

2 схема идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации;

3 схема идентификации с нулевой передачей знаний.

2.7 Для чего используется процедура “рукопожатия”:

**1 для взаимной проверки подлинности;**

2 для распределения ключей между подлинными партнерами;

3 для безопасного использования интеллектуальных карт.

2.8 Параллельная схема идентификации позволяет увеличить:

**1 число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации;**

2 регистрацию времени для каждого сообщения;

3 объект-эталон для идентификации и аутентификации пользователей.

2.9 Недостатки использования пароля для аутентификации

(Ответ считается верным, если отмечены все правильные варианты ответов.)

**1 сложность запоминания;**

**2 небольшой размер ключевой информации;**

3 погрешность аутентификации.

2.10 Достоинства биометрической аутентификации

(Ответ считается верным, если отмечены все правильные варианты ответов.)

**1 неотделимость биометрических признаков от дееспособной личности;**

**2 трудность фальсификации биометрических признаков;**

3 высокая стоимость оборудования для распознавания биометрических признаков.

2.11Многофакторной аутентификацией называется

1 аутентификация с использованием пароля;

2 аутентификация с использованием биометрического признака;

**3 аутентификация с использованием нескольких факторов.**

2.12 Простой аутентификацией является

**1 аутентификация с использованием пароля;**

2 аутентификация с использованием биометрического признака;

3 аутентификация с использованием USB-токена.

2.13 Примером двухфакторной аутентификации является

1 аутентификация по отпечатку пальца;

2 аутентификация по голосу;

**3 аутентификация по паролю и последующему вводу SMS-сообщения;**

4 аутентификация по паролю.

2.14 Примером двухфакторной аутентификации является

1 аутентификация по почерку;

2 аутентификация по голосу;

**3 аутентификация с USB-токеном с защитой доступа к данным и криптографическим функциям на основе PIN-кода;**

4 аутентификация по узору радужной оболочки и сетчатки глаза.

2.15 Способы защиты от подбора пароля

(Ответ считается верным, если отмечены все правильные варианты ответов)

**1 изменение пароля, установленного по умолчанию;**

**2 правила ограничения формата пароля;**

3 использование в качестве пароля известных цитат;

4 использование межсетевого экрана;

5 использование антивирусной программы;

**6 блокирование учетной записи после нескольких неспешных попыток аутентификации.**

2.16 Карта с магнитной полосой является реализацией фактора аутентификации…

1 на основе знания чего либо;

**2 на основе обладания чем-либо;**

3 на основе биометрических характеристик.

2.17 Реализацией фактора аутентификации на основе знания чего-либо является:

**1 PIN-код;**

2 OTP-токен, генерирующий одноразовый пароль;

3 отпечаток пальца;

**4 парольная фраза.**

2.18 Дополнительный фактор аутентификации на основе места проведения процедуры может быть реализован:

**1 с использованием смарт-карт интегрированных с RFID;**

2 с использованием цифровых сертификатов;

3 с использованием электронной подписи;

4 с использованием парольной фразы.

2.19 Согласно стандарту NCSC-TG-017 аутентификация на основе двух факторов- на основе знания чего-либо и на основе обладания чем-либо –кодируется следующим образом:

1 1;

**2 12;**

3 3;

4 123.

2.20 Код типа аутентификации 13 согласно стандарту NCSC-TG-017 соответствует:

1 аутентификации на основе знания чего-либо и на основе обладания чем-либо;

2 аутентификации на основе знания чего-либо ;

3 аутентификации на основе знания чего-либо и на основе на основе биометрических характеристик;

**4 аутентификации на основе знания чего-либо, на основе обладания чем-либо и на основе на основе биометрических характеристик.**

2.21 Аутентификация на основе хешированного пароля заключается в следующем:

**1 сервер аутентификации сравнивает результат вычисления однонаправленной функции *H* от введенного пользователем пароля с значением однонаправленной функции, хранящимся в учетной записи пользователя;**

2 сервер аутентификации находит учетную запись пользователя в базе данных аутентификации и сравнивает введенные данные с её содержимым;

3 аутентификация с помощью пароля для доступа к данным локального устройства, например, USB-токена.

2.22 Какой пароль является наиболее надежным

1 QWERTY123;

2 afgh;

3 34ak32rty;

**4 Ad12\_kL4.**

2.23 Метод аутентификации «запрос-ответ» на основе одноразовых паролей предполагает:

**1 генерацию одноразового пароля в результате шифрования закрытым ключом случайного числа, полученного от сервера аутентификации;**

2 вычисление одноразового пароля в результате шифрования закрытым ключом случайного числа, генерирующееся на основе предыдущего значения;

3 генерацию одноразового пароля в результате шифрования закрытым ключом текущего времени.

2.24 Для какого метода аутентификации на основе одноразового пароля характерна проблема «рассинхронизации» OTP-токена

(Ответ считается верным, если отмечены все правильные варианты ответов)

1 метод «запрос - ответ»;

**2 метод «синхронизация по времени»;**

**3 метод «только ответ»;**

**4 метод «синхронизация по событию».**

2.25 Для перехвата пароля пользователя при помощи программы-анализатора в локальной сети злоумышленнику нет необходимости:

**1 инсталлировать программу-анализатор на компьютер пользователя;**

2 иметь сетевое подключение к локальной сети пользователя;

**3 находиться в одном помещении с пользователем.**

2.26 Преимущества аутентификации типа "запрос-ответ" (пользователя на удаленном сервере) по сравнению с аутентификацией при помощи паролей заключаются в том, что:

**1 аутентификация может выполняться в открытой сети;**

**2 злоумышленник не может повторно использовать шифртекст, сгенерированный пользователем;**

3 имя пользователя передается в зашифрованном виде.

2.27 Серьезными проблемами аутентификации пользователя сервером при помощи пароля являются:

(Ответ считается верным, если отмечены все правильные варианты ответов)

**1 передача пароля пользователя по незащищенной сети;**

2 ошибки пользователя при вводе пароля;

**3 использование злоумышленником программы-анализатора.**

2.28 Защита от атак анализаторов возможна, если:

(Ответ считается верным, если отмечены все правильные варианты ответов)

**1 каждый пользователь шифрует свой пароль при помощи своего ключа шифрования, пароль каждого пользователя используется однократно;**

2 все пользователи шифруют свои пароли при помощи одного и того же ключа шифрования;

**3 каждый пользователь шифрует свой пароль и метку времени при помощи своего ключа шифрования.**

2.29 Система Kerberos позволяет:

(Ответ считается верным, если отмечены все правильные варианты ответов)

1 выполнять одностороннюю аутентификацию пользователя на удаленном сервере;

**2 выполнять взаимную аутентификацию между пользователем и сервером;**

**3 использовать один и тот же механизм проверки идентичности пользователя и сервера.**

**Список использованных источников**

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. –Введ. 2008-02-01 -М.: ФГУ «ГНИИ ПТЗИ ФСТЭК России», 2008. -12 с.
2. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф.Шаньгин.-М.: Радио и связь, 2001. -376с.
3. Рекомендации по обеспечению безопасности при разработке приложений Windows Azure». - Режим доступа: <http://docplayer.ru/65139-Rekomendacii-po-obespecheniyu-bezopasnosti-pri-razrabotke-prilozheniy-windows-azure.html>.
4. Административные правонарушения в области связи и информации: кодекс об административных правонарушениях (КоАП РФ) // Система ГАРАНТ. - Режим доступа: [http://base.garant.ru/12125267/13/#block\_1311 #ixzz3xPFQsBWd](http://base.garant.ru/12125267/13/#block_1311 ).
5. Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации: руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 21 с.
6. Ключевые особенности Astra Linux Special Edition по реализации требований безопасности информации. - Режим доступа: <http://www.astralinux.com> /klyuchevye-osobennosti.html
7. Операционная система МСВС с пакетом офисных и мультимедийных программ. - Режим доступа: <http://gistechnik.ru/pub/3-publik/65-mcbc.html>.
8. Дьяков, М. Глобальный взлом / М. Дьяков. - Режим доступа: http://www.banki.ru/news/daytheme/?id=6530329.
9. Обеспечение защиты мобильных устройств. - Режим доступа: http://www.leta.ru/services/information-security/mobile-security.html.
10. Мобильная безопасность: защита мобильных устройств в корпоративной среде [Электронный ресурс]//Хakep. –Режим доступа: <https://xakep.ru/2011/10/13/> 57058/
11. Продукты «Континент Т-10». –Режим доступа: http://www.securitycode.ru /products/kontinent\_t\_10/variants/
12. Лебедев, П. BYOD: когда производители откроют телефоны для криптозащиты? [Электронный ресурс] // П. Лебедев //Cnews. –Режим доступа: <http://www.cnews.ru/reviews/sredstva_zashchity_informatsii_i_biznesa_2013/articles/byod_kogda_proizvoditeli_otkroyut_telefony_dlya_kriptozashchity/>
13. Петрухин, В. Безопасность виртуальных сред[Электронный ресурс] / В. Петрухин// Открытые системы. – Режим доступа: [http://www.osp.ru/os/2011/04/ 13008785/](http://www.osp.ru/os/2011/04/%2013008785/)
14. Пичугов, К. Почему безопасность виртуальных инфраструктур нельзя обеспечить только традиционными средствами защиты? [Электронный ресурс]/К. Пичугов// Cnews. –Режим доступа: [http://www.securitycode.ru/upload/iblock/8e9/ CNEWS\_bezopasnost\_virtualizacii.pdf](http://www.securitycode.ru/upload/iblock/8e9/%20CNEWS_bezopasnost_virtualizacii.pdf).
15. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студ. высш. учеб. заведений. — М.: Академия, 2008.
16. Платонов, В.В. Программно-аппаратные средства защиты информации / В.В. Платонов: Академия, 2013. – 336 с.
17. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 21 с.
18. Гайдамаки, Н.А. Теоретические основы компьютерной безопасности[Электронный ресурс] / Н.А. Гайдамаки: учебное пособие. –Екатеринбург, 2008. -212 с. –Режим доступа: http://elar.urfu.ru/bitstream/10995/1778/5/ 1335332\_ schoolbook.pdf.
19. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин, Москва: ДМК Пресс, 2012. -592 с.
20. Аутентификация. Теория и практика обеспеxения безопасности доступа к информационным ресурсам: учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов [и др.]; Под ред. А. А. Шелупанова, С. Л. Груздева . —М.: Горячая линия—Телеком, 2009. — 552 с.:
21. NCSC-TG-017. A Guide to Understanding Identification and Authentication in Trusted Systems
22. Комплекс интеграции СЗИ НСД с системой видеомониторинга и контроля доступа «Рассвет-СВМиКД». –Режим доступа: <http://www.accord.ru/svm-rassvet.html>
23. Интеграция СЗИ НСД и СКУД. – Режим доступа: [http://www.okbsapr.ru/ svmikd.html](http://www.okbsapr.ru/%20svmikd.html).
24. Биометрические системы аутентификации. – Режим доступа: http://android-smartfon.ru/article/biometricheskie-sistemy-autentifikacii.
25. Lee Neely. Безопасность мобильных устройств. Часть 1 – Пароли и биометрическая аутентификация. – Режим доступа: <http://www.securitylab.ru/analytics/> 477982.php
26. Руководство пользователя для работы с системой «интернет-банк. – Режим доступа: https://www.rosbank.ru/files/dbo/docs/manual\_ib\_ind.pdf
27. Как использовать одноразовый пароль в Сбербанк ОнЛайн. – Режим доступа: <http://bankivonline.ru/publ/osbo/rukovodstvo/odnorazovyj_parol_v_sisteme_sberbank_onlajn/3-1-0-16>
28. Евтеев, Д. Как я перестал бояться токенов и полюбил одноразовые пароли / Д. Евтеев, С.В. Гордейчик // Защита информации. INSIDE № 5’2008. –Режим доступа: <http://www.ptsecurity.ru/download/PT-OTP-2008.pdf>
29. Полянская, О. Инфраструктура открытых ключей / О.Полянская. – Режим доступа: <http://www.intuit.ru/studies/courses/110/110/info>
30. Andreas Pashalidis, Chris J. Mitchell. A Taxonomy of Single Sign-On Systems.
31. Макушкин Ю. Основы операционных систем / Ю. Макушкин, Д.Зотов. – Режим доступа: http://www.intuit.ru/studies/courses/2192/31/lecture/998?page=5
32. Аутентификация, авторизация и управление доступом в операционных системах Windows и Unix (полная версия). – Режим доступа: <http://www.olifer.co.uk/new_rus/CN-5ed/cn5-aditions/auth-autor-OS.htm>
33. Лясин, Д.Н. Модель безопасности ОС Windows: методические указания к лабораторным работам / Сост. Д.Н. Лясин, С.Г. Саньков: Волгоград. гос. техн. ун-т. -Волгоград, 2011, – 24 с.
34. DACLs and ACEs. –Режим доступа: https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa446597(v=vs.85).aspx
35. Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты: методический документ ФСТЭК., 2013.
36. Авезова, Я.Э.Вопросы обеспечения доверенной загрузки в физических и виртуальных средах/ Я.Э. Авезова, А.А. Фадин // Вопросы кибербезопасности. №1(14) – 2016.
37. Как сбросить пароль BIOS на компьютере и ноутбуке. –Режим доступа: <http://itkompik.ru/remont-i-obsluzhivanie/kak-sbrosit-parol-bios.html>
38. UEFI - что это? –Режим жоступа: <http://www.nastrojkabios.ru/informatsiya-o-bios/o-uefi-i-bios.html>
39. UEFI FAQ. –Режим доступа: [http://4pda.ru/forum/index.php? showtopic=468127](http://4pda.ru/forum/index.php?%20showtopic=468127)
40. Берд Киви. UEFI: долгожданный наследник BIOS и заклятый друг Linux / К.Берд. – режим доступа: <http://www.3dnews.ru/618151>
41. Возможности ALTELL TRUST. –Режим доступа: [http://www.altell.ru/ products/trust/features/](http://www.altell.ru/%20products/trust/features/)
42. Шапиро, Л. Двухфакторная аутентификация в Службе Каталога AD DS /Л. Шапиров. –Режим доступа: <http://www.oszone.net/12469/>
43. ROHOS LOGON KEY. –Режим доступа: <http://www.rohos.ru/products/rohos-logon-key/>
44. Сабанова, А.Г. Классификация процессов аутентификации / А.Г. Сабанова // Вопросы защиты информации" (ВЗИ). - № 3, июнь, 2013.
45. Безмалый, В.Ф. Аппаратная аутентификация / В.Ф. Безмалый.–Режим доступа: <https://www.it-community.in.ua/2008/01/apparatnaya-autentifikatsiya.html/>
46. Биометрическая идентификация. –Режим доступа: <http://www.aladdin-rd.ru/solutions/bio/>
47. Технология биометрической аутентификации по отпечаткам пальцев. –Режим доступа: www.aladdin-rd.ru/support/downloads/get?ID=38969.
48. Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа: Наука и техника, Санкт-Петербург, 2004.
49. Духан, Е. И. Программно-аппаратные средства защиты компьютерной информации. практический курс:учебное пособие / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков;Екатеринбург: УрГУ, 2008, 240 с.
50. ГОСТ Р ИСО/МЭК27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. –Введ. 2006-27-12. -М.: 2008.
51. Dallas Lock 8.0. Руководство по эксплуатации. –Режим доступа: <https://www.dallaslock.ru/upload/medialibrary/cp/documents/RU.48957919.501410-02%2092%20-%20%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%BF%D0%BE%20%D1%8D%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D0%B8.pdf>
52. Шрамко, В. Аппаратно-программные средства контроля доступа[Электронный ресурс] / В. Шрамко // PCWEEK. –Режим доступа : <https://www.pcweek.ru/themes/detail.php?ID=63924>
53. IButton memory overview. – Режим доступа : <https://www.maximintegrated.com/en/products/ibutton/ibuttons/memoryoverview.cfm>
54. Новый обзор элктронных ключей-идентификаторов iButton от фирмы Dallas Semiconductor. – Режим доступа : [http://www.gaw.ru/html.cgi/txt/publ/other /ibutton.htm](http://www.gaw.ru/html.cgi/txt/publ/other%20/ibutton.htm).
55. Применение устройств iButton. – Режим доступа : <http://www.spd.net.ru/Article/iButton_review.aspx>
56. White Paper 8: 1-Wire® SHA-1 Overview. – Режим доступа : <https://www.maximintegrated.com/en/app-notes/index.mvp/id/1201>
57. Electronic Cash and User Authentication using the Dallas Semiconductor. Maxim DS1963S Monetary iButton. – Режим доступа : http://files.maximintegrated.com /sia\_bu/public/ecash\_sha\_tutorial.ppt
58. Smart Card & Security Basics. – Режим доступа : <http://www.smartcardbasics.com/pdf/7100030_BKL_Smart-Card-&-Security-Basics.pdf>
59. Рутокен. – Режим доступа :<https://www.rutoken.ru/products/all/rutoken-lite/#features>
60. Гусаров, Ю.В. Персональное средство криптографической защиты информации ШИПКА /Ю.В. Гусаров. – Режим доступа : <http://www.okbsapr.ru/gus3.html>
61. Рутокен эцп 2.0 flash. – Режим доступа :https://www.rutoken.ru /products/all/rutoken-ecp-flash/#use
62. eToken NG-FLASH (Java). – Режим доступа : <http://www.aladdin-rd.ru/catalog/etoken/flash/>
63. Статистика основных угроз безопасности в сетях ss7 мобильной связи. – Режим доступа: <https://www.ptsecurity.com/upload/ptru/analytics/SS7-Vulnerability-2016-rus.pdf>
64. Советкин. Что такое двухфакторная аутентификация и протокол FIDO U2F. – Режим доступа : <https://tproger.ru/articles/fido-u2f/>
65. FIDO UAF Architectural Overview. – Режим доступа :https://fidoalliance.org /specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.pdf
66. Universal 2nd Factor (U2F) Overview. – Режим доступа : <https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-overview-v1.1-id-20160915.pdf>
67. U2F Technical Overview. – Режим доступа : https://developers.yubico.com /U2F/Protocol\_details/Overview.html
68. JaCarta U2F для Online-аутентификации. – Режим доступа : <http://www.aladdin-rd.ru/catalog/jacarta_u2f/img/JaCarta_U2F_Obzornaya_presentazia_po%20productu.pdf>
69. Шауро, Е. Исследование устройств класса TrustScreen / Е. Шауро. – Режим доступа : <http://www.securitylab.ru/blog/personal/shaurojen/25164.php>
70. Федотенко, М. Доверенное устройство подтверждения в ДБО юридических лиц – удобство клиентов и защита от мошенничества. Вопросы внедрения / М. Федотенко. – Режим доступа : <http://www.securitylab.ru/analytics/485467.php>
71. Антифрод-терминал. – Режим доступа : <http://www.aladdin-rd.ru/catalog/antifraud/images/antifraud_pres.pdf>
72. Подписание платёжного поручения в системе ДБО. – Режим доступа : <http://developer.aladdin-rd.ru/antifraud_terminal/2.0/scenario/paymentsign.html>
73. Булдакова, Т.И. Оценка эффективности защиты систем электронного документооборота[Электронный документ] / Т.И. Булдакова, Б.В. Глазунов, Н.С. Ляпина// Доклады ТУСУРа, № 1 (25), часть 2, июнь 2012 – Режим доступа : <http://old.tusur.ru/filearchive/reports-magazine/2012-25-2/052.pdf>
74. Survival guides - TLS/SSL and SSL (X.509) Certificates. – Режим доступа : <http://www.zytrax.com/tech/survival/ssl.html>
75. Формат сертификатов открытых ключей X.509. – Режим доступа : <http://www.inssl.com/x509-open-key-specifications.html>
76. Обзор форматов стандарта CAdES. – Режим доступа : <https://www.strozhevsky.com/free_docs/CAdES.pdf>
77. КриптоПро ЭЦП. – Режим доступа : <https://www.cryptopro.ru/products/cades>
78. Горбатов, B.C. Основы технологии PKI/ B.C. Горбатов, О.Ю. Полянская. - М.: Горячая линия - Телеком, 2004. - 248 с.
79. D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang Introduction to Public Key Technology and the Federal PKI Infrastructure.
80. Инфраструктуры открытых ключей. – Режим доступа : <http://www.intuit.ru/studies/courses/110/110/lecture/27989?page=1>
81. Краткое руководство по Microsoft PKI. – Режим доступа : <http://www.cyberguru.ru/operating-systems/windows-admin/microsoft-pki.html>
82. Обеспечение безопасности PKI: планирование иерархии ЦС. – Режим доступа : https://msdn.microsoft.com/ru-ru/library/dn786436(v=ws.11).aspx.