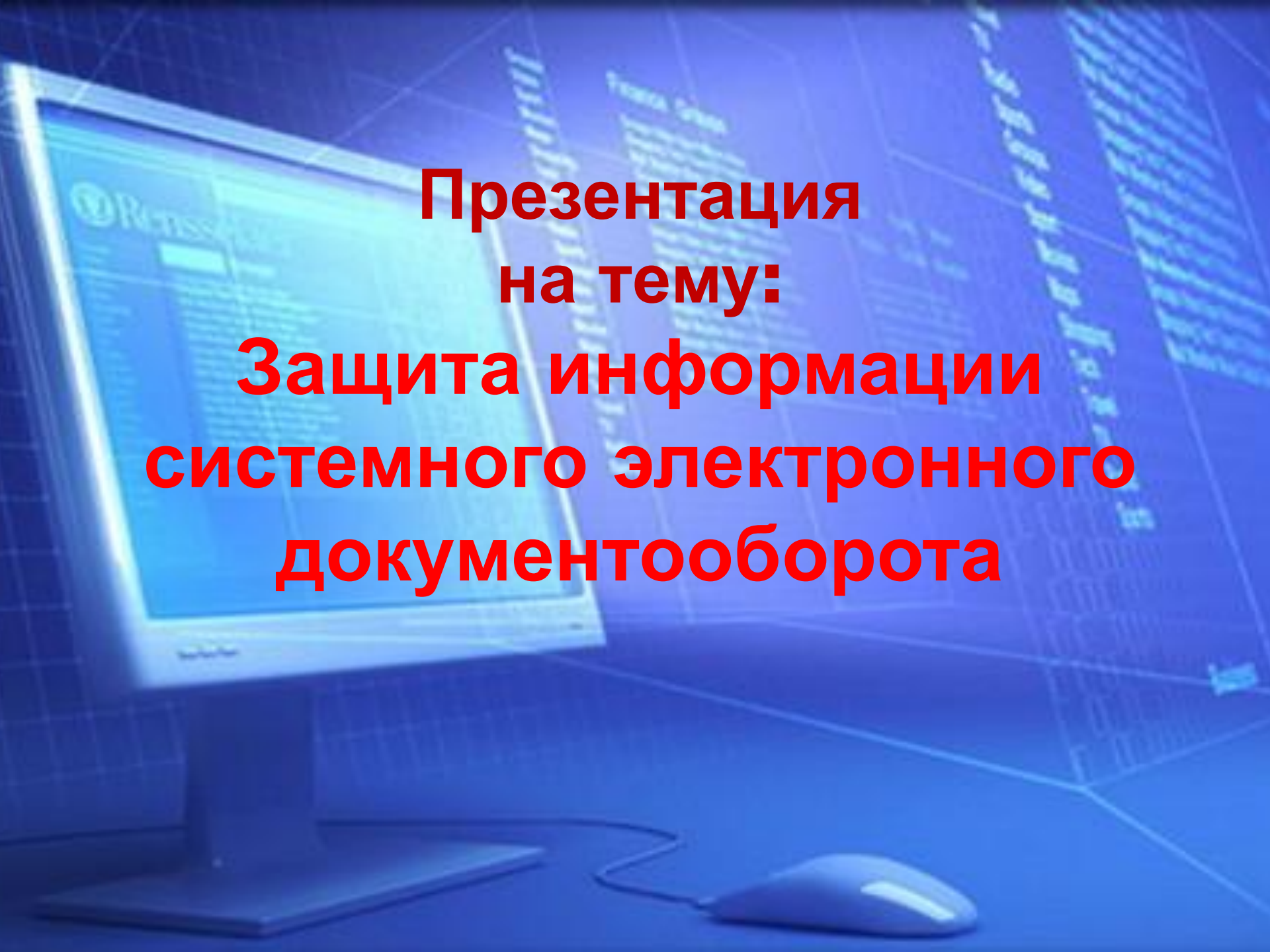

Презентация
на тему:
Защита информации
системного электронного
документооборота

30 ноября отмечается Международный день защиты информации.

Информация и знания: две валюты, которые никогда не выходили из моды.

Основные понятия защиты информации и информационной безопасности

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты вашей информации.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и получения защищаемой информации

Достоверность информации – свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого

Общая структура системы обеспечения защиты информации

Система защиты информации — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Вводимая информация должна быть авторизована, полна, точна и должна подвергаться проверкам на ошибки. Необходимо проверять точность информации с помощью процедур сравнения результатов обработки с предполагаемыми

Одним из методов защиты информации является создание физической преграды пути злоумышленникам к защищаемой информации (если она хранится на каких-либо носителях).

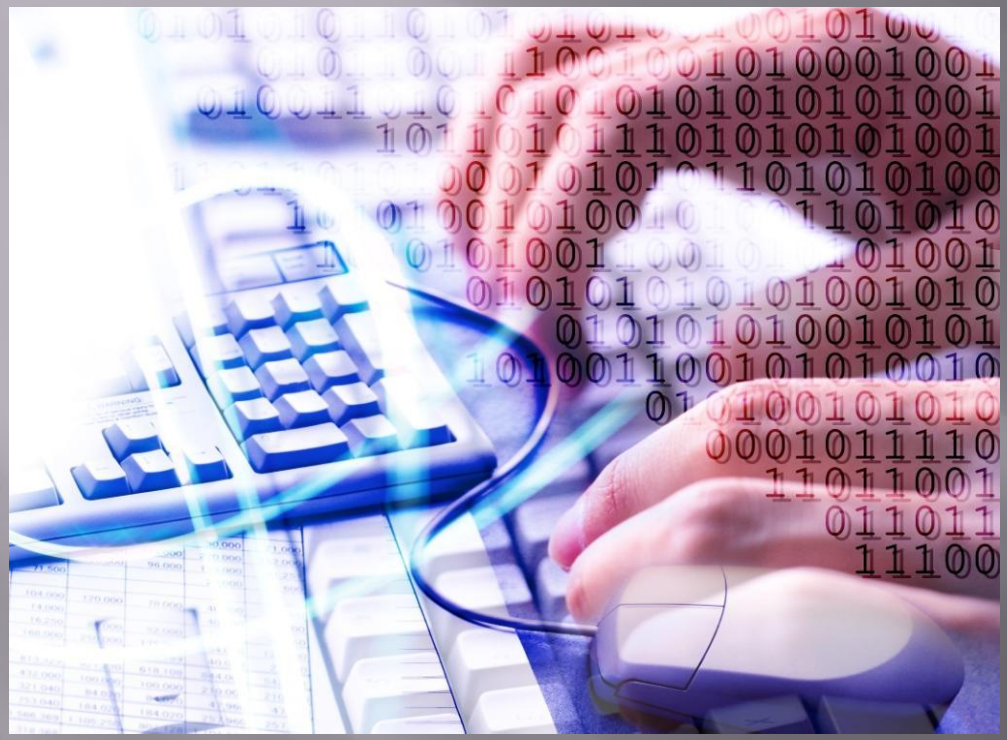
Пароли - один из типов идентификации - что-то, что знает только пользователь. Двумя другими типами идентификации, которые тоже эффективны, является что-то, чем владеет пользователь (например, магнитная карта), или уникальные характеристики пользователя (его голос).

Захватчик паролей -- это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы.

Системный подход к построению системы защиты, означающий оптимальное сочетание взаимосвязанных организационных, программных,. аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям.

ЗАЩИТА ИНФОРМАЦИИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА



Проблема безопасной и гарантированной доставки электронных документов ныне актуальна как никогда.

Управление доступом – это методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.


Управление доступом включает следующие функции защиты:
Идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора)
Опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору
Регистрацию (протоколирование) обращений к защищаемым ресурсам
Разрешение и создание условий работы в пределах установленного регламента
Реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети).

Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением. Голография представляет собой раздел науки и техники, занимающийся изучением и созданием способов, устройств для записи и обработки волн различной природы.

Как и всякий объект, информация обладает свойствами.

Маскировка -- метод защиты информации с использованием инженерных, технических средств, а также путем криптографического закрытия информации.

Установка препятствия -- метод физического преграждения пути злоумышленнику к защищаемой информации, в т.ч. попыток с использованием технических средств съема информации и воздействия на нее.

Не всегда такие средства информационной безопасности как VPN и простое шифрование данных для повседневной работы оказывается удобным и приемлемым. Известны случаи, когда самые изощрённые системы защиты были бесполезны, так как их непосредственным пользователям было просто лень ими пользоваться из-за непривычности, неудобства, нежелания учиться новому функционалу.

Как известно, информация - это самый ценный товар. Современные «злоумышленники» (агенты иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, психически больные лица и др.) не будут, подобно Бене Крику, «брать банк» - им это не надо. Достаточно стать специалистом в области компьютерных технологий и похитить этот самый ценный товар - информацию.

Как известно, информация - это самый ценный товар. Современные «злоумышленники» (агенты иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, психически больные лица и др.) не будут, подобно Бене Крику, «брать банк» - им это не надо. Достаточно стать специалистом в области компьютерных технологий и похитить этот самый ценный товар - информацию.

Электронный документооборот (ЭДО)

Электронный документооборот — это единый механизм по работе с документами, представленными в электронном виде, с реализацией концепции «безбумажного делопроизводства».

Система электронного документооборота

Система (ЭДО) –это автоматизированная многопользовательская система, сопровождающая процесс управления работой иерархической организации с целью обеспечения выполнения этой организацией своих функций. При этом предполагается, что процесс управления опирается на человеко-читаемые документы, содержащие в слабоформализованной форме инструкции для сотрудников организации, необходимые к исполнению.

Преимущества электронного документооборота.

Возникает возможность полностью отказаться от бумажных документов при условии, что это не противоречит действующему законодательству (некоторые типы документов требуется иметь в бумажном виде). Это позволяет избежать дублирования информации на различных носителях, обеспечивает надежное хранение данных и предотвращает утечку конфиденциальной

Отпадает надобность в физической передаче сотрудникам бумажных документов, что многократно ускоряет процессы принятия решений по документам и доведения решений руководства до сотрудников.

Электронная цифровая подпись (ЭЦП)

ЭЦП — это аналог собственноручной подписи человека, применяемый в электронных документах. Электронно-цифровая подпись создается с помощью закрытого ключа — уникальной последовательности символов, которая известна его владельцу и предназначена для создания ЭЦП в электронных документах с использованием соответствующих средств.

Использование ЭЦП во всем жизненном цикле электронного документа — при его создании, согласовании, утверждении, ознакомлении с ними.

Пример цифровой электронной подписи

Стандартный набор угроз системного электронного документооборота.

Естественно, передаваемые в электронном виде документы имеют различную степень конфиденциальности и могут содержать сведения от полностью открытых до являющихся коммерческой тайной самого предприятия или его партнеров.

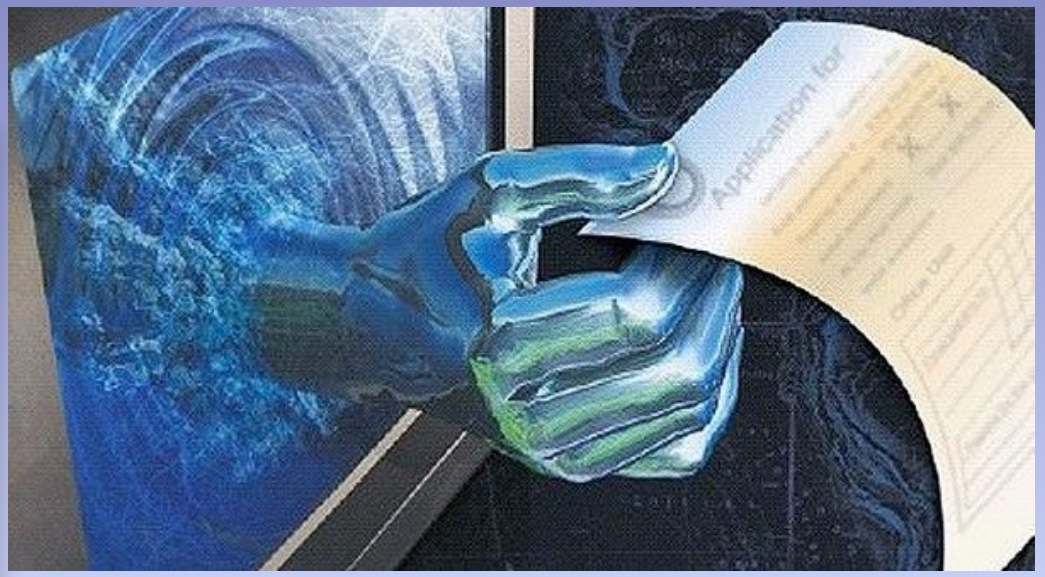
```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Угрозы для системы электронного документооборота достаточно
стандартны и могут быть классифицированы следующим образом.

Угроза целостности — повреждение и уничтожение информации,
искажение информации — как не намеренное в случае ошибок и сбоев,
так и злоумышленное.

Угроза конфиденциальности — это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменения маршрутов следования.

Проблема защиты информации путем ее видоизменения, делающего невозможным ее прочтение посторонним лицом, волновала человечество издревле. История криптографии - ровесница истории человеческого языка

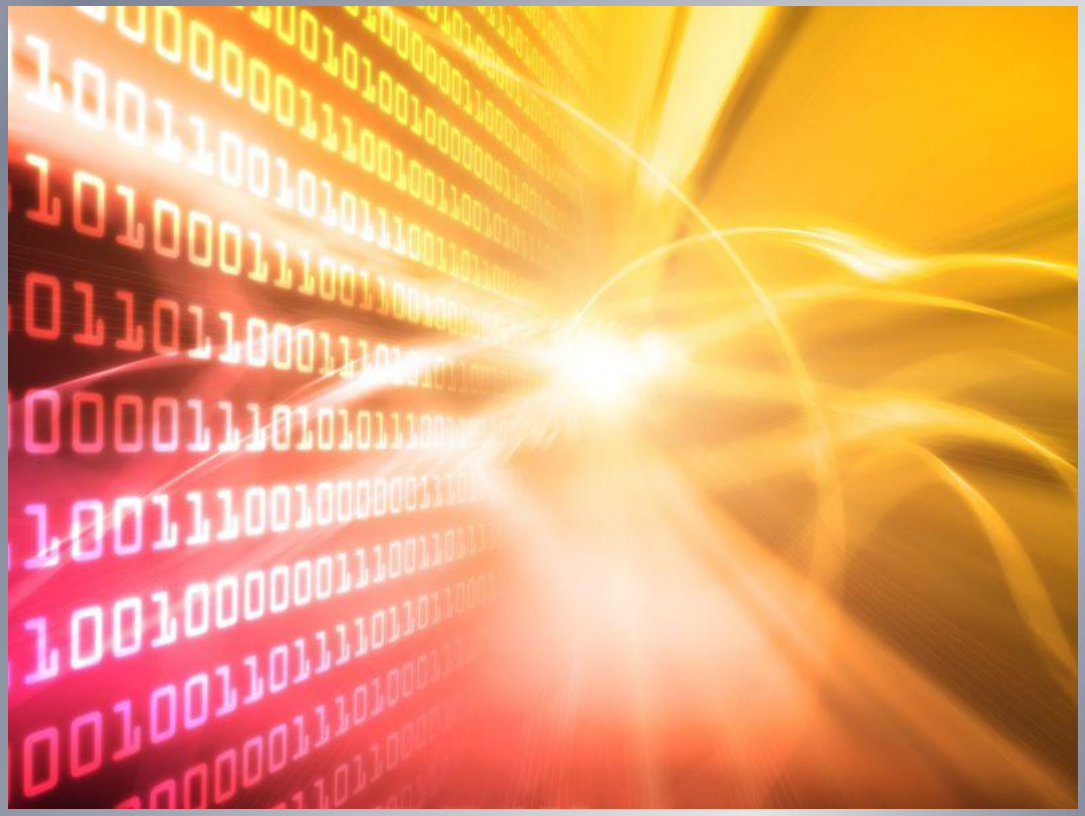


В современной российской рыночной экономике обязательным условием успеха предпринимателя в бизнесе, получения прибыли и сохранения целой и невредимой организационной структуры является обеспечение экономической безопасности его деятельности. Одна из главных составных частей экономической безопасности - информационная безопасность.

Защищенный документооборот нужен сегодня на всех уровнях госуправления. Другое дело – на всех ли этих уровнях необходима юридическая значимость электронных документов? В первую очередь она нужна для документов, которые могут иметь правовые последствия

Угрозы для системы электронного документооборота достаточно стандартны и могут быть классифицированы следующим образом. Угроза целостности - повреждение и уничтожение информации, искажение информации - как не намеренное в случае ошибок и сбоев, так и злоумышленное. Угроза конфиденциальности - это любое нарушение конфиденциальности, в том числе кража, перехват информации, изменения маршрутов следования. Угроза работоспособности системы - всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы; сюда входят как умышленные атаки, так и ошибки пользователей, а также сбои в оборудовании и программном обеспечении.

Защиту именно от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота. При этом, с одной стороны, внедряя СЭД, упорядочивая и консолидируя информацию, увеличиваются риски реализации угроз, но с другой стороны, как это ни парадоксально, упорядочение документооборота позволяет выстроить более качественную систему защиты.

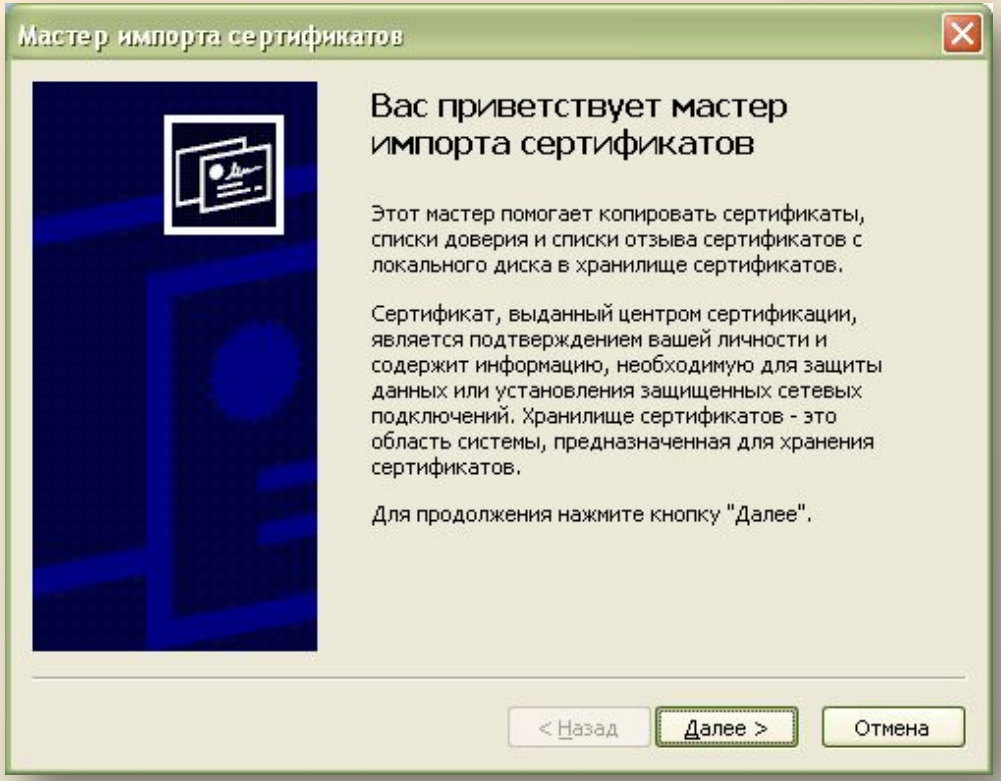


Основное проблемное место при организации защиты СЭД, как отмечают большинство разработчиков систем защиты, это не технические средства, а лояльность пользователей. Как только документ попадает к пользователю, конфиденциальность этого документа по отношению к пользователю уже

Подход к защите электронного документооборота должен быть комплексным. Необходимо трезво оценивать возможные угрозы и риски СЭД и величину возможных потерь от реализованных угроз. Как уже говорилось, защиты СЭД не сводится только лишь к защите документов и разграничению доступа к ним.

Основное отличие в системах защиты - это алгоритмы, применяемые в шифровании и ЭЦП К сожалению, пока вопрос защищенности систем документооборота только начинает интересовать конечных пользователей и разработчиков соответственно.

Для обеспечения безопасного обмена открытыми ключами между пользователями информационной системы используются



Сертификат представляет собой структуру данных, которая содержит открытый ключ владельца сертификата и подписана электронной цифровой подписью его издателя. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей.

Всякая информация в машине или системе требует той или иной защиты, под которой понимается совокупность методов, позволяющих управлять доступом выполняемых в системе программ к хранящейся в ней информации.

«Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения».

«Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Надежность защиты информации может быть оценена временем, которое требуется на расшифрование (разгадывание) информации и определение ключей.

Обеспечение защиты информации от несанкционированного доступа – дело сложное, требующее широкого проведения теоретических и экспериментальных исследований по вопросам системного проектирования.

«Кто владеет информацией — тот владеет миром.»

Натан Ротшильд

«Люди чаще думают, чем говорят, а из-за этого теряется много информации.» ***Бернар Вербер***

«Информация — наиболее ценный из известных мне товаров.»

Уолл-Стрит.

Информация — основная валюта демократии.

Спасибо за внимание!

Презентацию подготовил:
студент гр. БПИЗК-02
Давлетбаев А.