Содержание:

ВВЕДЕНИЕ

Мы живём в веке постоянных изменений и обновлений информационных систем и технологий. Компьютеризация современного общества дошла до такой черты, когда буквально вся информация - книги, рабочие документы, фото и видеофайлы, данные предприятий, а также личная информация хранятся на компьютерах. Информация обрабатывается и подвергается угрозам ежесекундно, следовательно, особую роль сегодня стремительно занимает исследование вопроса о сохранении персональных данных от посторонних лиц и информационных угроз.

Проблема защиты информации является одной из самых важных на сегодняшний день, поэтому тема данного исследования: "Виды и состав угроз информационной безопасности" является одной из самых актуальных в настоящее время.

Основной целью работы является изучение темы видов и состава угроз информационной безопасности.

Для достижения указанной цели необходимо решить задачи:

- рассмотреть основные понятия информационной безопасности;
- рассмотреть виды и состав информационной безопасности;
- рассмотреть основные способы защиты информации;
- изучить криптографическую защиту информации.

Объектом исследования являются виды и состав угроз информационной безопасности.

Предметом данного исследования являются теоретические и практические аспекты в области изучения проблем угроз информации.

Теоретическая значимость состоит, прежде всего, в расширении и углублении научных представлений о видах и составе угроз информационной безопасности. Сформулированные в работе положения и выводы развивают и дополняют ряд теории информационной безопасности.

Практическая ценность полученных результатов заключается в анализе статистических данных и изучении классификации угроз информационной безопасности.

Работа включает в себя: введение, основную часть, состоящую из двух глав, заключение, список использованных источников, а также приложение.

Во введении обосновываются актуальность выбранной темы, излагаются цели и задачи исследования, объект и предмет исследования, теоретическая и практическая значимость исследования, приводиться характеристика основных источников информации.

В первой главе рассмотрены основные понятия информационной безопасности, что такое информация, информационная безопасность, информационная угроза, а также виды, состав и классификация угроз информационной безопасности.

Вторая глава посвящена основным способам и средствам защиты информации, также рассмотрены технологии обеспечения безопасности и тема криптографии.

В заключении сделаны выводы по исследованиям работы.

В списке использованных источников содержится перечень документов, использованных при выполнении данной работы. Приводятся источники и книги, на которые ссылается данная работа.

В приложении представлена практическая часть на тему исследование проблем защиты информации.

При исследовании данной темы были проанализированы научные труды Степанова Е.А. по теме "Информационная безопасность и защита информации", а также работы Ракова А.С. на тему "Информационная безопасность телекоммуникационных систем и сетей".

Таким образом, данная тема особо актуальна в настоящее время и ей стоит уделить особое внимание.

Глава 1. Угроза информационной безопасности

1.1. Основные понятия информационной безопасности

Первым делом стоит рассмотреть основные понятия темы информационной безопасности.

Информация есть сведения, передаваемые людьми в устной и письменной форме, а также информация - это результат обработки и отражения многообразия окружающего нас мира, это сведения об предметах и явлениях природы, деятельности других людей[1].

Информационная безопасность представляет собой свойство защищенности системы от случайного или неслучайного вмешательства в нормальный процесс её функционирования, от попыток хищения (несанкционированного доступа) информации, модификации или физическою разрушения ее компонентов, то есть способность системы противодействовать различным возмущающим воздействиям и угрозам извне[2].

Угроза информационной безопасности представляют собой действия, попытки или события, приводящие к разрушению, искажению или несанкционированному использованию ресурсов системы, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства[3].

Таким образом, были рассмотрены основные понятия темы информационной безопасности.

Далее необходимо рассмотреть виды, состав и классификацию угроз информационной безопасности.

1.2. Классификация угроз информационной безопасности

В настоящее время известно множество видов угроз информационной безопасности и данные угрозы информационной безопасности могут быть классифицированы по различным признакам[4].

Необходимо рассмотреть основные шесть видов угроз информационной безопасности[5]:

- раскрытие конфиденциальной информации;
- взлом (вмешательство в систему извне);
- вывод системы из строя, снижение работоспособности;
- превышение полномочий непривилегированных пользователей;
- отказ от авторства и транзакций;
- уничтожение и искажение информации.

Основные шесть видов угроз информационной безопасности представлены на рисунке 1[6].

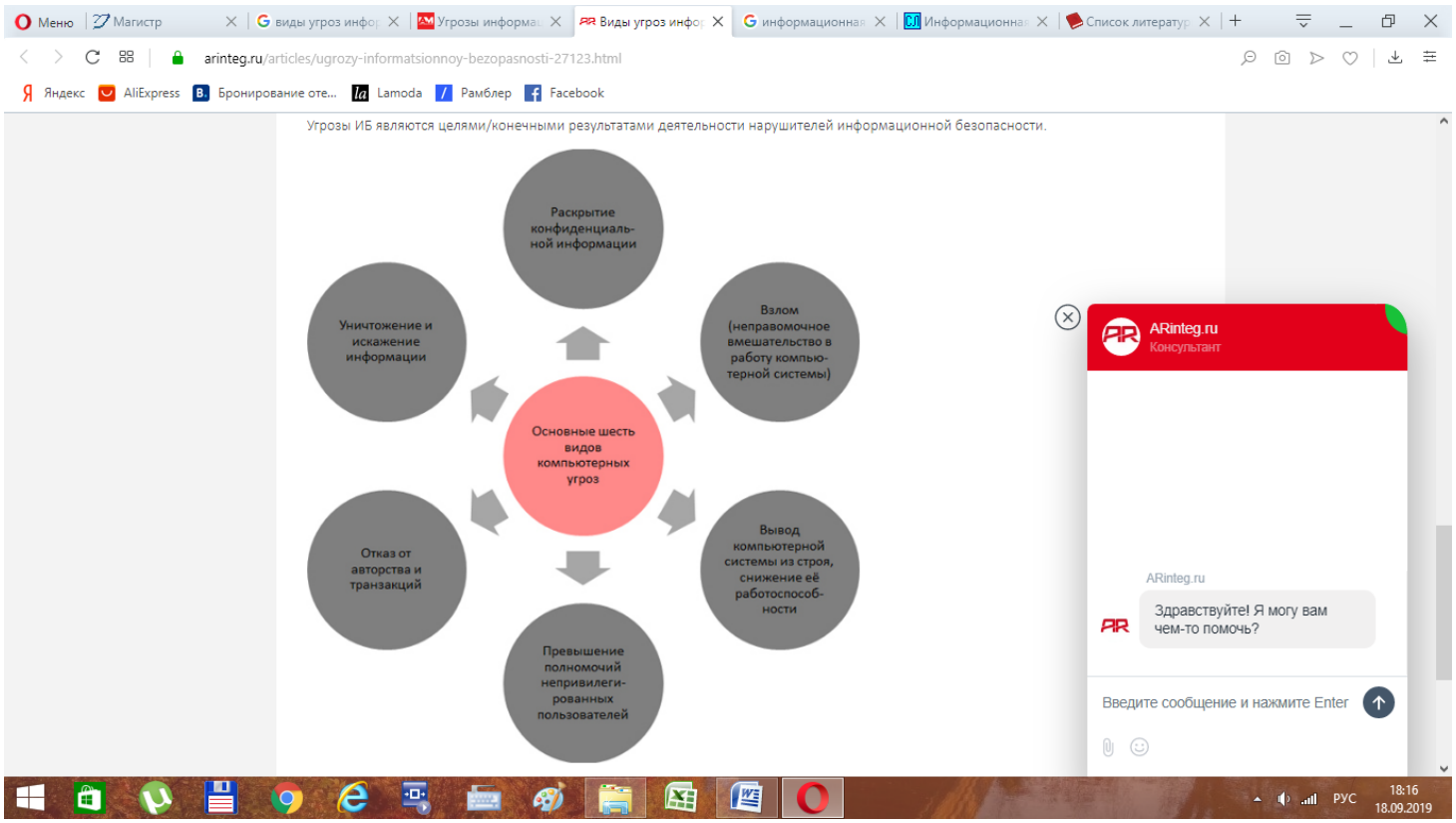


Рисунок 1. Виды угроз информационной безопасности

Далее необходимо рассмотреть классификацию угроз информационной безопасности.

По аспекту информационной безопасности угрозы бывают:

- угрозы конфиденциальности (неправомерный доступ к информации);
- угрозы целостности (неправомочное изменение данных);

- угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы)[7].

По степени преднамеренных действий:

- случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия);
- неслучайные (умышленные действия, например, шпионаж и диверсии)[8].

По расположению источника угрозы:

- внешние (источники угроз находятся вне системы);
- внутренние (источники угроз располагаются внутри системы)[9].

По размерам наносимого вреда:

- общие (нанесение объекту ущерба);
- локальные (причинение вреда отдельным частям объекта);
- частные (причинение вреда отдельным свойствам элементов объекта)[10].

По степени воздействия на информационную систему:

- активные (структура и содержание системы подвергается изменениям);
- пассивные (структура и содержание системы не подвергаются изменениям)[11].

Все источники угроз можно разделить на внешние и внутренние.

К внешним источникам угроз относятся:

- компьютерные вирусы и вредные программы;
- организации и отдельные лица;
- стихийные и природные бедствия и катаклизмы.

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами или вредоносными программами;
- несанкционированный доступ к персональной информации;
- информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
- действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;

- природные аварии, пожары, техногенные катастрофы[12].

К внутренним источникам угроз относятся:

- сотрудники организации;
- программное обеспечение;
- аппаратные средства.

Формами проявления внутренних угроз являются:

- ошибки пользователей и системных администраторов;
- нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;
- ошибки в работе программного обеспечения;
- отказы и сбои в работе компьютерного оборудования[13].

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

- информационные;
- программные;
- физические;
- радиоэлектронные;
- организационно-правовые[14].

К информационным угрозам относят:

- несанкционированный доступ к информационным ресурсам;
- незаконное копирование данных в информационных системах;
- хищение информации из библиотек, архивов, банков и баз данных;
- нарушение технологии обработки информации;
- противозаконный сбор и использование информации;
- использование информационного оружия.

К программным угрозам относят:

- использование ошибок и "дыр" в программном обеспечении;
- компьютерные вирусы и вредоносные программы;
- установка "закладных" устройств.

К физическим угрозам относят:

- уничтожение или разрушение средств обработки информации и связи;
- хищение носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты данных;
- воздействие на персонал.

К радиоэлектронным угрозам относят:

- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К организационно-правовым угрозам относят:

- закупки несовершенных или устаревших информационных технологий и средств информатизации;
- нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере.

Таким образом, в первой главе были подробно рассмотрены основные понятия информационной безопасности, а также классификация угроз информационной безопасности. Далее стоит рассмотреть основные способы и средства информационной безопасности.

Глава 2. Методы и средства защиты информации

2.1. Основные способы защиты информации

Развитие информационных систем и технологий, их применение во всех сферах человеческой жизнедеятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными и одновременно с этим более сложными. Чтобы защитить информацию, необходимо знать основные способы защиты информации. Для этого необходимо рассмотреть способы и средства защиты информации, которые представлены на рисунке 2[15].

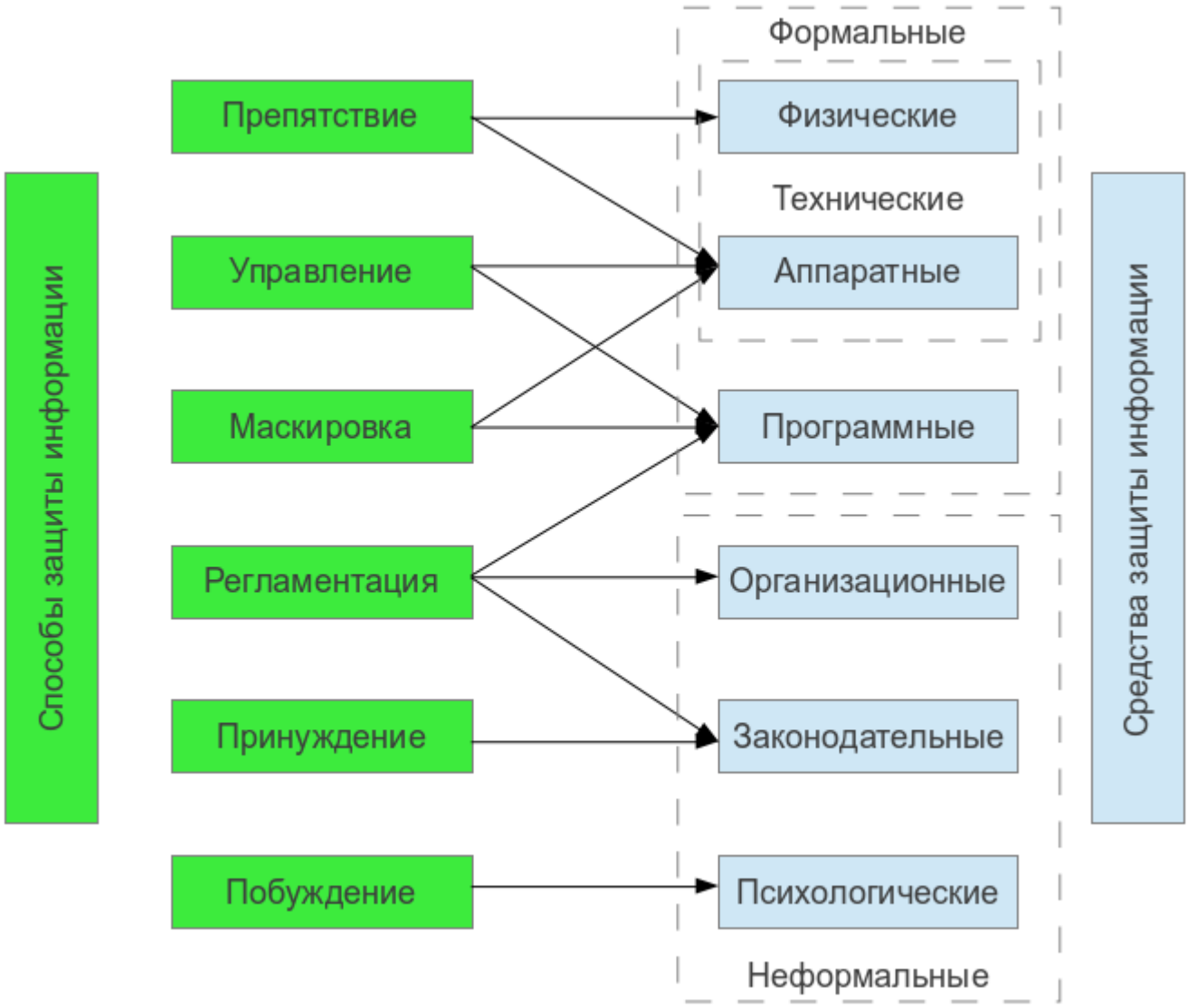


Рисунок 2. Способы и средства защиты информации

Перечислим основные способы защиты информации[16]:

1. препятствие есть метод физического преграждения пути злоумышленнику к информации;
2. управление доступом представляет собой способ защиты информации, который заключается в регулировании использования всех ресурсов компьютерной информационной системы.

Управление доступом включает такие функции защиты, как:

- идентификация пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

- проверка полномочий, то есть проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту;
- разрешение и создание условий работы в пределах установленного регламента;
- регистрация (протоколирование) обращений к защищаемым ресурсам;
- регистрация (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий;

1. маскировка - это метод защиты информации путём её криптографического закрытия. При передаче информации по каналам связи большой протяженности данный метод является единственно надёжным;
2. регламентация - метод защиты информации, при котором возможности несанкционированного доступа сводятся к минимуму;
3. принуждение - метод защиты информации, заключающийся в том, что пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации, чтобы не подвергнуться материальной, административной или уголовной ответственности;
4. побуждение - метод защиты информации, который побуждает пользователя и персонал системы не нарушать установленный порядок за счёт соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Далее стоит рассмотреть средства защиты информации[17]:

1. физические средства представляют собой механические, электрические, электромеханические, электронные, электронно-механические устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов;
2. аппаратные средства - различные электронные и электронно-механические устройства, схемно-встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации;
3. программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации. Из средств программного обеспечения системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография - это наука об обеспечении секретности и аутентичности (подлинности) передаваемых сообщений;
4. организационные средства - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с

целью решения задач защиты информации;
5. законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности;
6. психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

При использовании любой информационной системы и технологии следует обратить внимание на наличие средств защиты данных. Безопасность данных включает обеспечение достоверности данных и защиту данных и программ от несанкционированного доступа, копирования, изменения.

Достоверность данных контролируется на всех этапах технологического процесса эксплуатации электронных информационных систем. Различают визуальные и программные методы контроля.

Визуальный контроль выполняется на домашинном и заключительном этапах. При этом обязателен контроль при вводе данных, их корректировке, то есть везде, где есть вмешательство пользователя в вычислительный процесс. Контролируются отдельные реквизиты, записи, группы записей, файлы.

Программные методы контроля достоверности данных выполняется на внутримашинном этапе и закладываются на стадии рабочего проектирования.

Защита данных и программ от несанкционированного доступа, копирования, изменения реализуется программно-аппаратными методами и технологическими приёмами.

К программно-аппаратным средствам защиты относят пароли, электронные ключи, электронные идентификаторы, электронную подпись, средства кодирования, декодирования данных. Для кодирования, декодирования данных, программ и электронной подписи используются криптографические методы. Например, в США применяется криптографический стандарт, разработанный группой IETF. Экспорту он не подлежит. Разработаны в том числе и отечественные электронные ключи, например, Novex Key для защиты программ и данных в системах Windows, DOS, Netware. Средства защиты аналогичны, по словам специалистов, дверному замку.

Замки взламываются, но никто не убирает их с двери, оставив квартиру открытой.

Технологический приём заключается в организации многоуровневой системы защиты программ и данных как средствами проверки паролей, электронных подписей, электронных ключей, скрытых меток файла, использованием программных продуктов, удовлетворяющих требованиям компьютерной безопасности, так и методами визуального и программного контроля достоверности, целостности, полноты данных.

Безопасность обработки данных зависит от безопасности использования компьютерных систем. Компьютерной системой называется совокупность аппаратных и программных средств, различного рода физических носителей информации, собственно данных, а также персонала, обслуживающего перечисленные компоненты.

В настоящее время в США разработан стандарт оценок безопасности компьютерных систем - критерии оценок пригодности. В нём учитываются четыре типа требований к компьютерным системам:

- требования к проведению политики безопасности - security policy;
- ведение учёта использования компьютерных систем - accounts;
- доверие к компьютерным системам;
- требования к документации.

Требования к проведению последовательной политики безопасности и ведение учёта использования компьютерных систем зависят друг от друга и обеспечиваются средствами, заложенными в систему, то есть решение вопросов безопасности включается в программные и аппаратные средства на стадии проектирования. Нарушение доверия к компьютерным системам, как правило, бывает вызвано нарушением культуры разработки программ: отказом от структурного программирования, неисключением заглушек, неопределенным вводом. Для тестирования на доверие нужно знать архитектуру приложения, правила устойчивости его поддержания, тестовый пример. Требования к документации означают, что пользователь должен иметь исчерпывающую информацию по всем вопросам. При этом документация должна быть лаконичной и понятной.

Только после оценки безопасности компьютерной системы она может поступить на рынок.

Во время эксплуатации информационной системы наибольший вред и убытки приносят вирусы. Защиту от вирусов можно организовать так же, как и защиту от несанкционированного доступа. Технология защиты является многоуровневой и содержит следующие этапы:

1. Входной контроль нового программного обеспечения, который осуществляется группой специально подобранных детекторов, ревизоров и фильтров. Например, в состав группы можно включить Scan, Aidstest, TPU8CLS. Можно провести карантинный режим. Для этого создается ускоренный компьютерный календарь. При каждом следующем эксперименте вводится новая дата и наблюдается отклонение в старом программном обеспечении. Если отклонения нет, то вирус не обнаружен.
2. Сегментация жесткого диска. При этом отдельным разделам диска присваивается атрибут Read Only. Для сегментации можно использовать, например, программу Manager.
3. Систематическое использование резидентных, программ-ревизоров и фильтров для контроля целостности информации, например Check21, SBM, Antivirus2.
4. Архивирование. Ему подлежат и системные, и прикладные программы. Если один компьютер используется несколькими пользователями, то желательно ежедневное архивирование. Для архивирования можно использовать PKZIP.

Эффективность программных средств защиты зависит от правильности действий пользователя, которые могут быть выполнены ошибочно или со злым умыслом. Поэтому следует предпринять следующие организационные меры защиты:

- общее регулирование доступа, включающее систему паролей и сегментацию винчестера;
- обучение персонала технологии защиты;
- обеспечение физической безопасности компьютера и магнитных носителей;
- выработка правил архивирования;
- хранение отдельных файлов в шифрованном виде;
- создание плана восстановления винчестера и испорченной информации.

Для шифровки файлов и защиты от несанкционированного копирования разработано много программ, например Catcher, Exeb. Одним из методов защиты является скрытая метка файла: метка (пароль) записывается в сектор на диске, который не считывается вместе с файлом, а сам файл размещается с другого сектора, тем самым файл не удается открыть без знания метки.

Следующим пунктом будет рассмотрена криптографическая защита информации.

2.2. Криптографическая защита информации

Для начала определим понятие криптография. Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает "тайнопись") зародилась как способ скрытой передачи сообщений[18].

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трёх главных проблем защиты данных:

- обеспечение конфиденциальности;
- целостности;
- подлинности передаваемых или сохраняемых данных.

Для обеспечения безопасности данных необходимо поддерживать три основные функции:

- защиту конфиденциальности передаваемых или хранимых в памяти данных;
- подтверждение целостности и подлинности данных;
- аутентификацию абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путём взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легальность (аутентичность), предоставляются разрешенные виды сетевого обслуживания[19].

Обеспечение конфиденциальности, целостности и подлинности, передаваемых и сохраняемых данных осуществляется, прежде всего, правильным использованием криптографических способов и средств защиты информации. Основой большинства криптографических средств защиты информации является шифрование данных[20].

Под шифром понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Под зашифровыванием информации понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифр-текст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют расшифровыванием (дешифрованием)[21].

Обобщенная схема криптосистемы шифрования показана на рисунке 3. Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования Ек с получением в результате шифр-текста С:

$C=Ek_i(Nf)$ (1)

где-параметр функции Е - ключом шифрования.

Рисунок 3. Обобщенная схема криптосистемы шифрования

Шифр-текст С, называемый также криптограммой, содержит исходную информацию М в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования кх.

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами)[22].

Обратное преобразование информации выглядит следующим образом:

$M' = Dk_i(C)$ (2)

Функция D является обратной к функции E и производит расшифровывание шифр-текста. Она также имеет дополнительный параметр в виде ключа K2. Ключ расшифровывания K2 должен однозначно соответствовать ключу K1 в этом случае полученное в результате расшифровывания сообщение M’ будет эквивалентно M. При отсутствии верного ключа K2 получить исходное сообщение M’ = M с помощью функции D невозможно.

С древних времён перед людьми стояла довольно сложная задача - убедиться в достоверности важных сообщений. Придумывались речевые пароли, сложные печати и замки. Рассмотрим самое раннее применение криптографии. В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы.

Возьмём известную всем пословицу о науке "Без наук как без рук" и зашифруем её. Данная пословица шифруется в таблице, состоящей из 4 строк и 4 столбцов (Таблица 1).

Таблица 1

Шифрование пословицы: "Без наук как без рук"

Б	**А**	**А**	**З**
Е	**У**	**К**	**Р**
З	**К**	**Б**	**У**

Н К Е К

Для получения шифрованного сообщения текст считывается по строкам и группируется по 4 буквы:

БААЗ ЕУКР ЗКБУ НКЕК

Вторая глава была посвящена основным способам и средствам защиты информации, также рассмотрены технологии обеспечения безопасности и тема криптографии, приведены примеры применения криптографии.

В конце данного исследования в Приложении представлена практическая часть курсовой работы, которая представляет собой инструкцию по практическому применению темы защиты информации. Рассмотрен порядок использования персонального ключевого носителя и проверка наличия электронного сертификата на персональном ключевом носителе и его срока действия для пользователя на предприятии ООО "Газпром трансгаз Самара" филиала "Управление материально-технического снабжения и комплектации".

ЗАКЛЮЧЕНИЕ

Мы живём в современном мире, где ежедневно обновляются и меняются информационные системы и технологии. Компьютеризация применяется во всех сферах человеческой деятельности. Информация ежесекундно подвергается угрозам. Следовательно данная тема исследования защиты информации занимает исследование сегодня особую роль.

Основной целью работы являлось изучение темы видов и состава угроз информационной безопасности.

Для достижения указанной цели были решены следующие задачи:

- рассмотрены основные понятия информационной безопасности;
- рассмотрены виды и состав информационной безопасности;
- рассмотрены основные способы защиты информации;
- изучена криптографическая защита информации.

Объектом исследования являлись виды и состав угроз информационной безопасности.

Предметом данного исследования являлись теоретические и практические аспекты в области изучения проблем угроз информации.

Теоретическая значимость состояла, в изучении научной информации о видах и составе угроз информационной безопасности.

Практическая ценность полученных результатов заключалась в анализе статистических данных и изучении классификации угроз информационной безопасности, а также теме криптографии.

Работа включает в себя: введение, основную часть, состоящую из двух глав, заключение, список использованных источников, а также приложение.

Во введении обосновываются актуальность выбранной темы, излагаются цели и задачи исследования, объект и предмет исследования, теоретическая и практическая значимость исследования, приводиться характеристика основных источников информации.

В первой главе рассмотрены основные понятия информационной безопасности, что такое информация, информационная безопасность, информационная угроза, а также виды, состав и классификация угроз информационной безопасности.

Вторая глава посвящена основным способам и средствам защиты информации, также рассмотрены технологии обеспечения безопасности и тема криптографии.

В заключении сделаны выводы по исследованиям работы.

В списке использованных источников содержится перечень документов, использованных при выполнении данной работы. Приводятся источники и книги, на которые ссылается данная работа.

В приложении представлена практическая часть на тему исследование проблем защиты информации.

При исследовании данной темы были проанализированы научные труды Степанова Е.А. по теме "Информационная безопасность и защита информации", а также работы Ракова А.С. на тему "Информационная безопасность телекоммуникационных систем и сетей".

Таким образом, цель решена, задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Информация, свободный. - Загл. с экрана.

Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Информационная_безопасность, свободный. - Загл. с экрана.

Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности, свободный. - Загл. с экрана.

1. Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Криптография, свободный. - Загл. с экрана.
2. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. - СПб. : СПбГУ ИТМО, 2015. - 98 с.

Гришина Н. В. Аутентификация. Учебное пособие / Н.В. Гришина. - М. : Форум, 2015. - 240 с.

Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах: моногр. / П.Н. Девянин. - М. : ИЛ, 2016. - 176 с.

Емельянова Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М. : Форум, 2015. - 368 с.

Емельянова Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М. : Форум, 2017. - 368 с.

1. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М. : ГЛТ, 2018. - 558 с.

Конотопов М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М. : КноРус, 2014. - 136 с.

1. Конотопов М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2016. - 136 с.
2. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2017. - 372 с.

Максименко В. Н. Защита информации в сетях сотовой подвижной связи / В.Н. Максименко, В.В. Афанасьев, Н.В. Волков. - М. : Горячая линия - Телеком, 2014. - 360 с.

Мельников Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М. : Флинта, 2014. - 448 с.

1. Семененко В.А. Информационная безопасность / В.А. Семененко. - М. : МГИУ, 2016. - 277 с.

Спесивцев А.В. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков. - М. : Радио и связь, 2016. - 192 с.

1. Урсул А. Д. Проблема информации в современной науке. - М. : Наука, 2017.
2. Чипига А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М. : Гелиос АРВ, 2017. - 336 с.

Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М. : "ДМК пресс. Электронные книги", 2014. - 592 с.

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М. : Книжный мир, 2017. - 352 с.
2. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. - М. : Академический проект, 2018. - 544 с.

ПРИЛОЖЕНИЕ

Инструкции по порядку использования персонального ключевого носителя

и проверке наличия сертификата на персональном ключевом носителе и его срока действия для пользователя

Рассмотрим предприятие ООО "Газпром трансгаз Самара". Доступ работников ООО "Газпром трансгаз Самара" к информационным системам и технологиям осуществляется по персональному уникальному имени (учетная запись

пользователя) на основе двухфакторной аутентификации с использованием персонального электронного ключа (смарт-карта eToken). Для входа в операционную систему персонального компьютера пользователь должен подключить ключ к считывающему устройству и ввести PIN-код (личный пароль). Порядок использования персонального ключевого носителя приведен в данной работе. После подключения ключа необходимо проверить наличие сертификатов и срока их действия.

Практической частью данного исследования являются инструкции по порядку использования персонального ключевого носителя и проверке наличия сертификата и его срока действия для пользователя.

Инструкции представляют собой порядок и способ осуществления доступа работников к информационным ресурсам данного предприятия, требования к PIN-коду и его смене, права и обязанности пользователей. Проверка наличия сертификатов на персональном ключевом носителе выполняется в программе SafeNet Authentication Client, которая предназначена для обеспечения работы USB-ключей и смарт-карт eToken (рисунок 4).

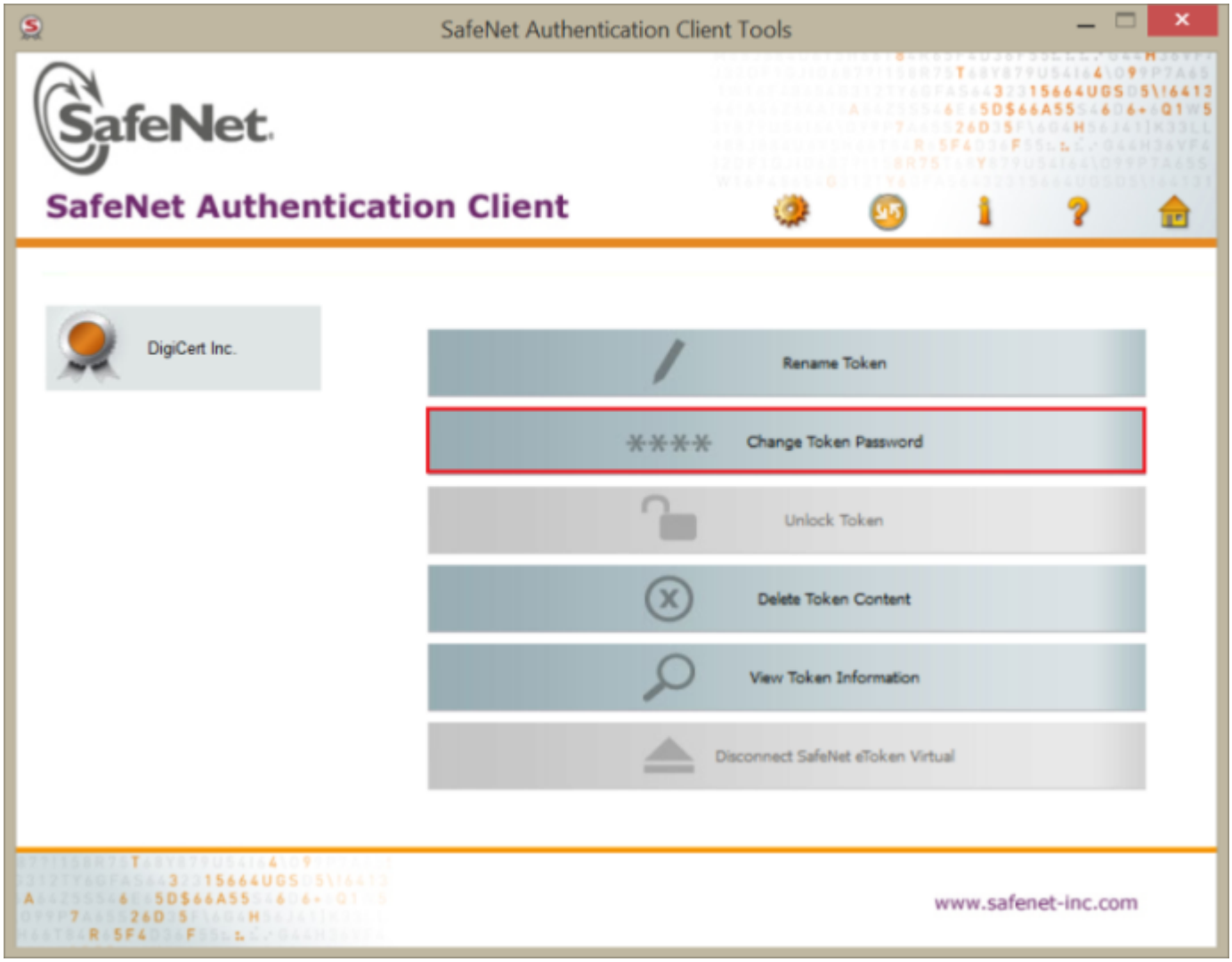


Рисунок 4. SafeNet Authentication Client

Порядок использования персонального ключевого носителя.

Доступ работников ООО "Газпром трансгаз Самара" к сервисам и информационным ресурсам организуется по персональному уникальному имени (учетная запись пользователя) на основе двухфакторной аутентификации с использованием персонального электронного ключа.

В качестве персонального электронного ключа используется смарт-карта (eToken) (рисунок 5).

Рисунок 5. Смарт-карта (eToken)

Для входа в операционную систему персонального компьютера и подключению к информационным ресурсам, пользователь должен подключить персональный электронный ключ eToken к считывателю компьютера и ввести PIN-код (рисунок 6).

Рисунок 6. Подключение персонального носителя к считывателю

Требования к PIN-коду и его смене

- pin-код должен быть известен только лично пользователю. допускается запись pin-кода на бумажном носителе при условии хранения таких носителей в личном сейфе (сейфе начальника подразделения) в запечатанном конверте, подписанном работником;
- длина pin-кода - не менее 6 (шесть) символов;
- в pin-коде должны присутствовать символы как минимум 3 категорий из 4 предложенных;
- заглавные буквы английского алфавита (a-z);
- строчные буквы английского алфавита (a-z);
- цифры (0-9);
- символы, не принадлежащие к алфавитно-цифровому набору (@, #, $, &, *);
- минимальное количество цифр в pin-коде - 2;

- минимальное количество специальных символов в pin-коде - 2;
- pin-код не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии) общепринятые сокращения (эвм, user), позиционные сочетания клавиш клавиатуры (qwerty);
- смена pin-кода не реже 1 раза в квартал;
- при смене pin-кода их значения не должны повторять ранее использованные комбинации и должны отличаться от предыдущего не менее чем в 4 позициях;
- при последовательном пятикратном неправильном вводе pin-кода персональный ключевой носитель блокируется;
- pin-код должен меняться пользователем самостоятельно не реже 1 раза в квартал, а также немедленно, в случае их компрометации (подозрения на его компрометацию). под компрометацией понимается утрата пользователем доверия к тому, что используемые pin-код недоступен посторонним лицам;
- первоначально выданный пользователю pin-код (12qw!@) используется разово и при первом входе в систему должен быть заменен на новый, известный только пользователю;
- порядок смены pin-кода приведен в пункте 6.

Обязанности Пользователей:

- обеспечить физическую сохранность персонального ключевого носителя и не допускать его утери;
- хранить в тайне pin-код;
- соблюдать требования по сложности pin-кода, по его периодической смене;
- в случае компрометации (подозрении на компрометацию) pin-кода незамедлительно сообщить в отдел по защите информации службы безопасности;

Действия, запрещенные Пользователям:

- хранить pin-код в доступных другим лицам местах;
- разглашать pin-код своего электронного ключа etoken (разглашение pin-кода ведет к компрометации учетной записи);
- передавать кому-либо электронный ключ etoken. только так можно быть уверенным, что никто не сможет действовать в среде обработки информации от вашего имени;
- оставлять электронный ключ etoken подключенным к рабочей станции при покидании рабочего места. несоблюдение этого правила может привести к тому, что в отсутствие пользователя можно воспользоваться его электронным

ключом etoken;

Ответственность Пользователей:

- пользователи несут ответственность за сохранность персонального ключевого носителя и считывателя электронного ключа etoken;
- процедура смены pin-кода;
- для смены pin-кода нужно щелкнуть правой кнопкой по значку "etoken pki client" (рисунок 7).

Рисунок 7. Значок "eToken PKI Client"

- в появившемся меню выбрать Изменить пароль eToken/ ChangeeTokenPassword (рисунок 8).

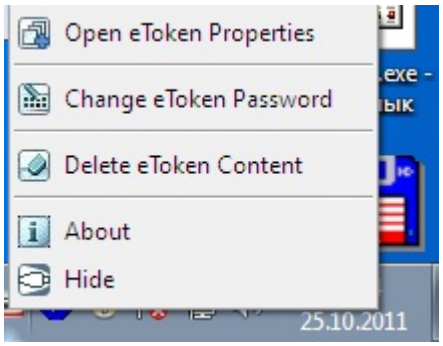


Рисунок 8. Смена пароля

- в появившемся окне введите текущий PIN-код (верхнее поле), новый PIN-код (среднее поле) и Подтверждение нового PIN-кода (нижнее поле). После этого нажимаем на кнопку "OK" и входим в систему с использованием нового PIN-кода (рисунок 9).

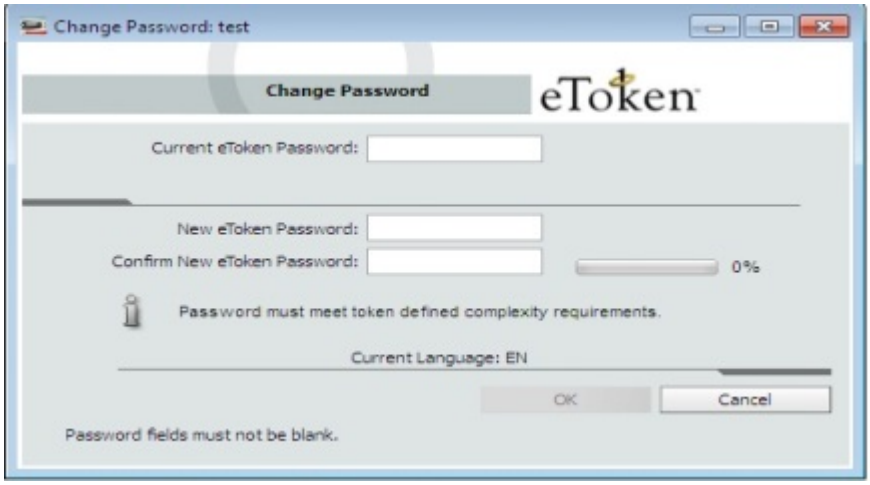


Рисунок 9. Порядок смены PIN-кода

Порядок использования персонального ключевого носителя рассмотрен.

Инструкция по проверке наличия сертификата на смарт-карте и его срока действия для пользователя

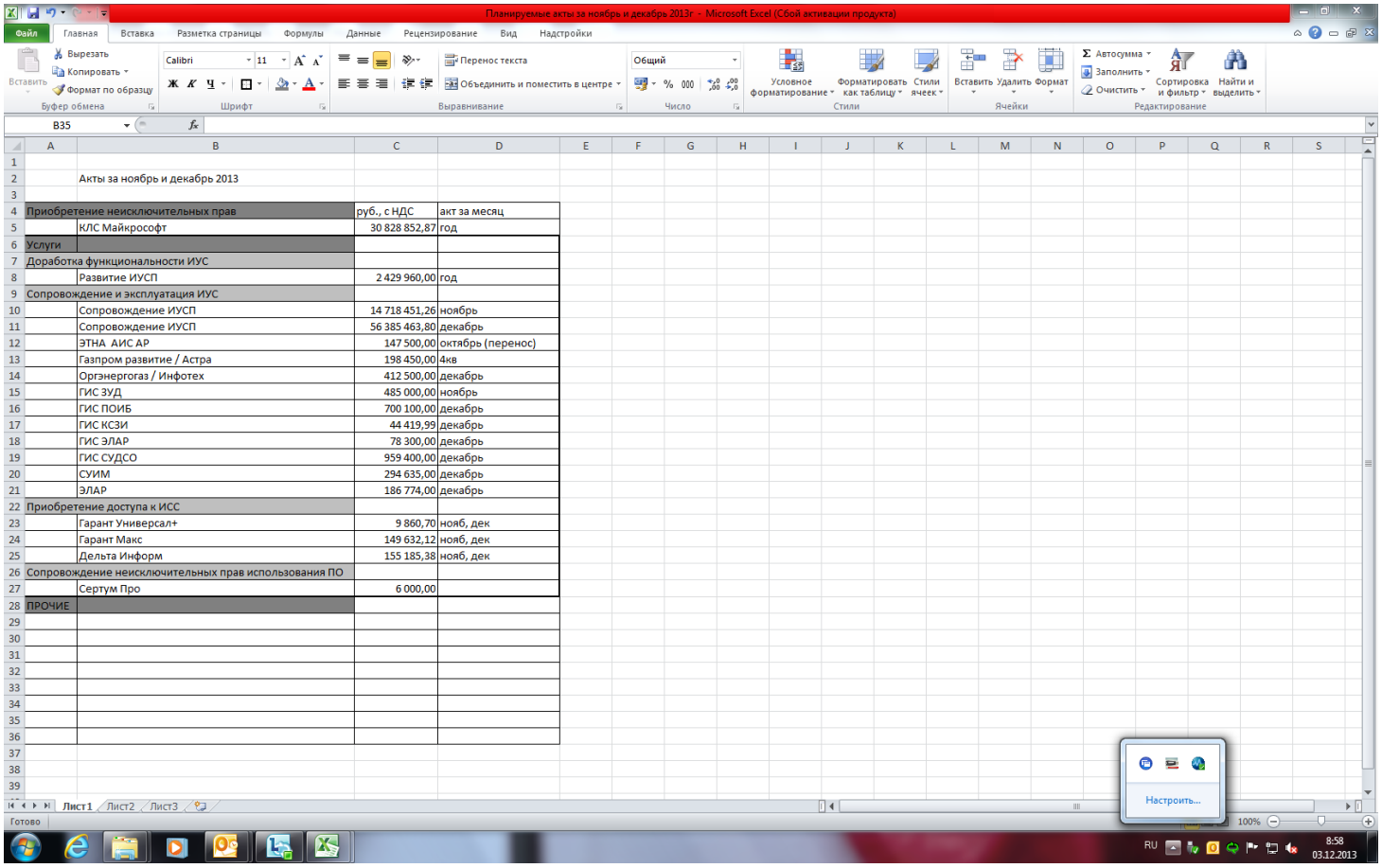
Для того чтобы проверить имеется ли на смарт-карте сертификат и какой его срок действия, необходимо сделать следующее:

- вставить интересующую нас смарт-карту в считыватель (рисунок 10).

Рисунок 10. Подключение персонального носителя к считывателю

- запустить "eToken PKI Client". Нажать правой кнопкой мыши на значок

в правом нижнем углу экрана, как показано на рисунке 11.



Планируемые акты за ноябрь и декабрь 2013г - Microsoft Excel (Сбой активации продукта)

Акты за ноябрь и декабрь 2013

Приобретение неисключительных прав	руб., с НДС	акт за месяц
КЛС Майкрософт	30 828 852,87	год
Услуги		
Доработка функциональности ИУС		
Развитие ИУСП	2 429 960,00	год
Сопровождение и эксплуатация ИУС		
Сопровождение ИУСП	14 718 451,26	ноябрь
Сопровождение ИУСП	56 385 463,80	декабрь
ЭТНА АИС АР	147 500,00	октябрь (перенос)
Газпром развитие / Астра	198 450,00	4кв
Оргэнергогаз / Инфотех	412 500,00	декабрь
ГИС ЗУД	485 000,00	ноябрь
ГИС ПОИБ	700 100,00	декабрь
ГИС КСЗИ	44 419,99	декабрь
ГИС ЭЛАР	78 300,00	декабрь
ГИС СУДСО	959 400,00	декабрь
СУИМ	294 635,00	декабрь
ЭЛАР	186 774,00	декабрь
Приобретение доступа к ИСС		
Гарант Универсал+	9 860,70	нояб, дек
Гарант Макс	149 632,12	нояб, дек
Дельта Информ	155 185,38	нояб, дек
Сопровождение неисключительных прав использования ПО		
Сертум Про	6 000,00	
ПРОЧИЕ		

Рисунок 11. Запуск "eToken PKI Client"

- выбрать "Открыть eTokenProperties" (рисунок 12).

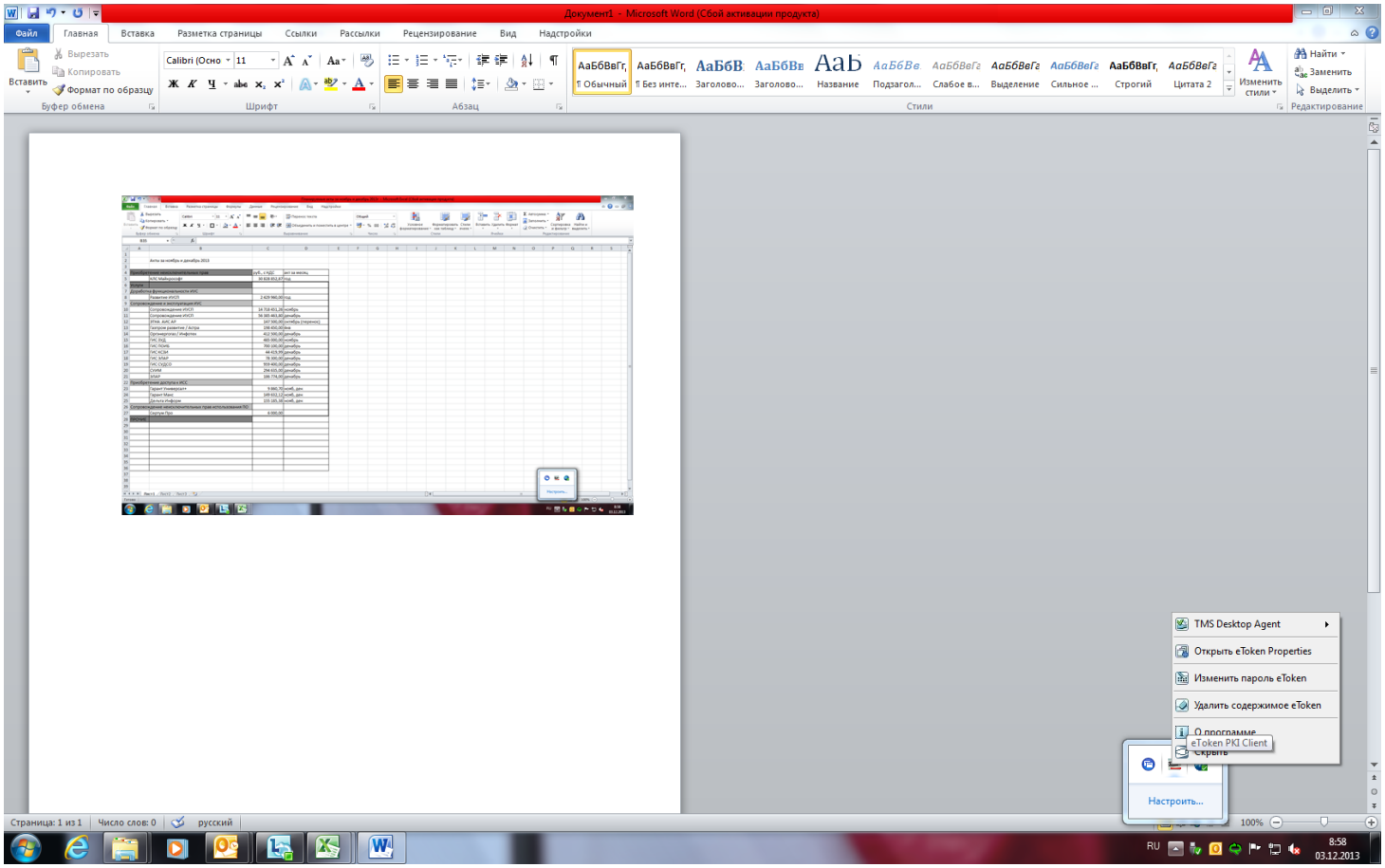


Рисунок 12. Выбор "Открыть eTokenProperties"

- появится окно программы (рисунок 13).

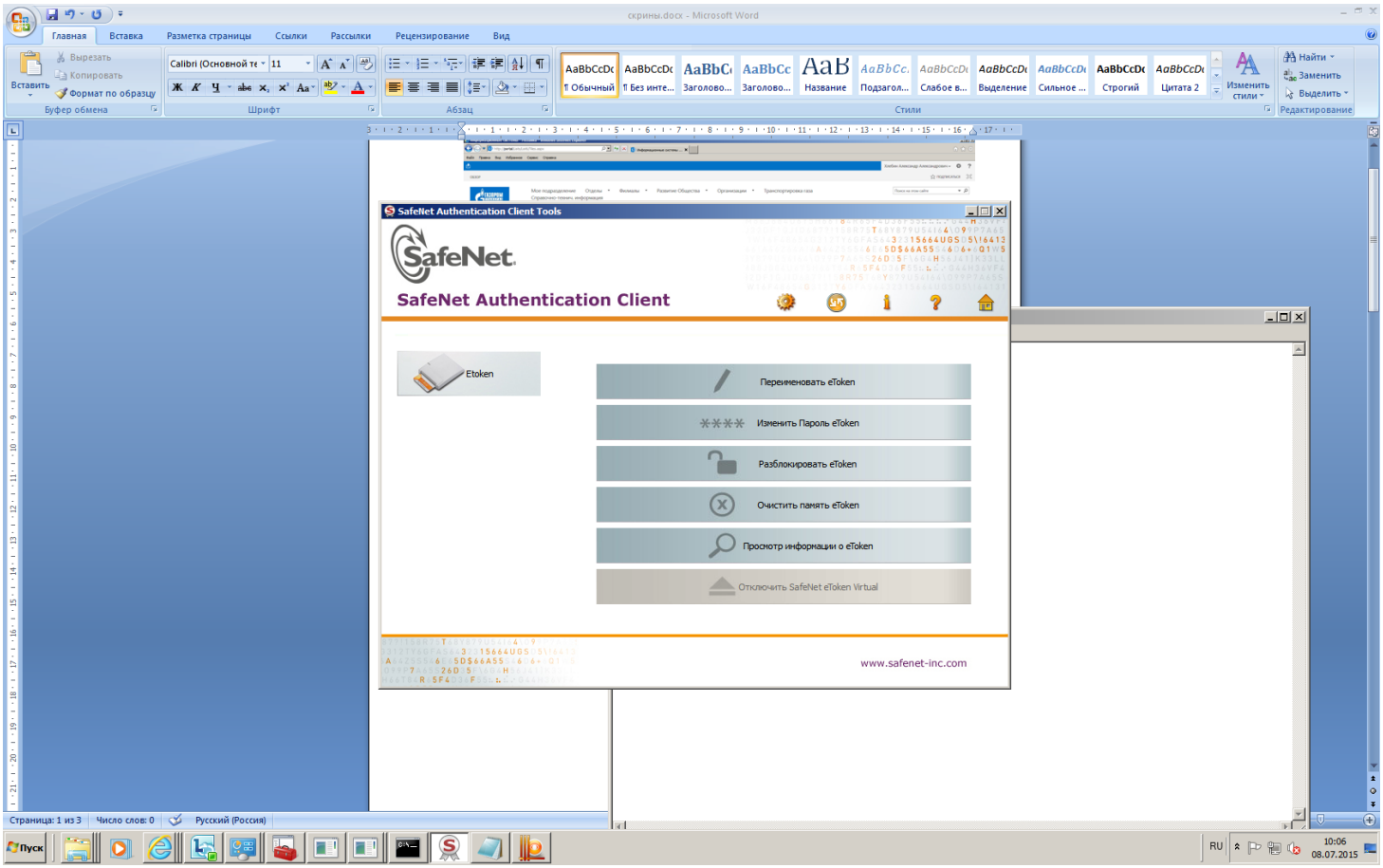


Рисунок 13. Окно программы " SafeNet Authentication Client"

- выбрать пункт "AdvancedView" или "Подробный вид" (значок ) (рисунок 14).

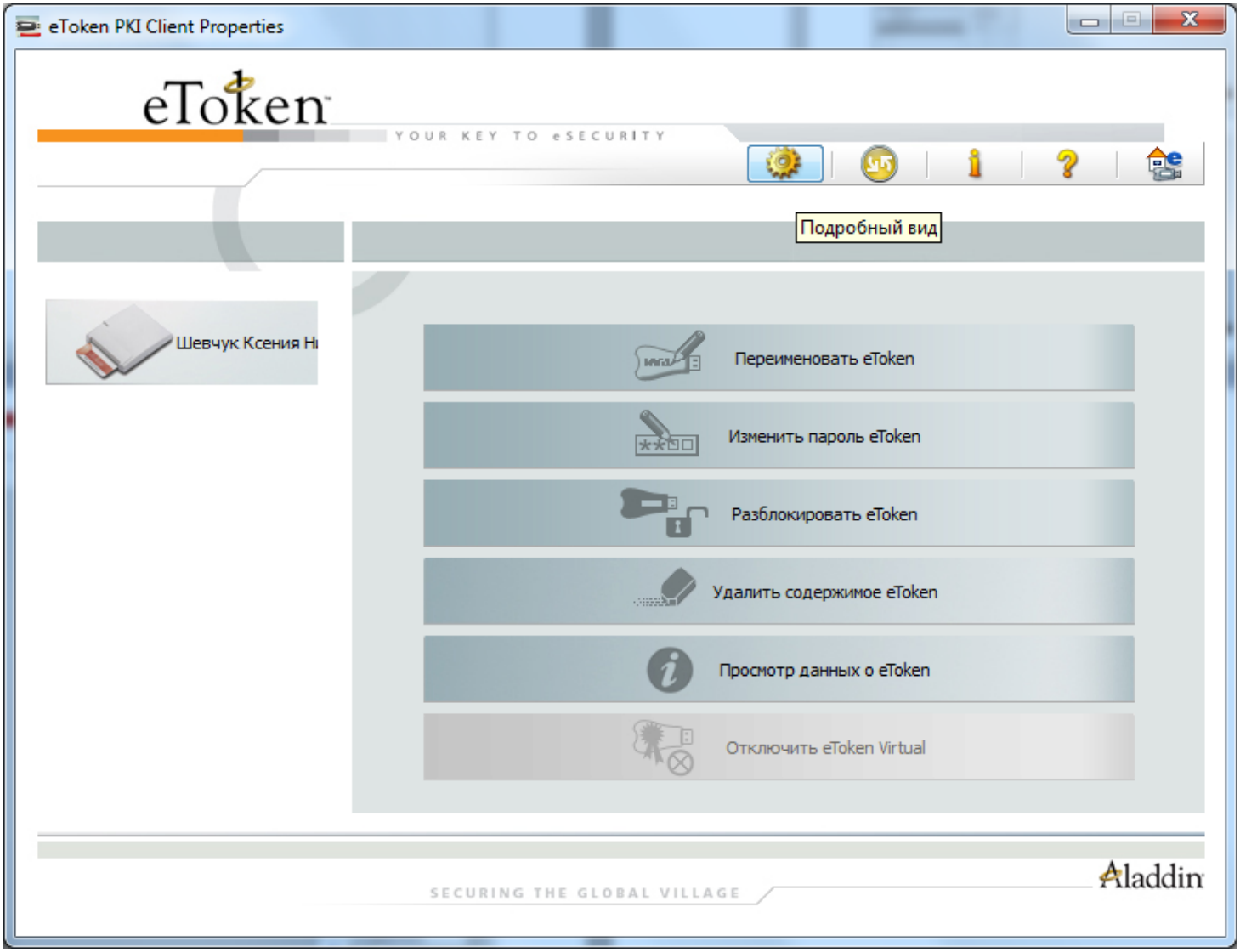


Рисунок 14. Выбор пункта "Подробный вид"

- если на смарт-карте имеются сертификаты, они будут показаны (рисунок 15).

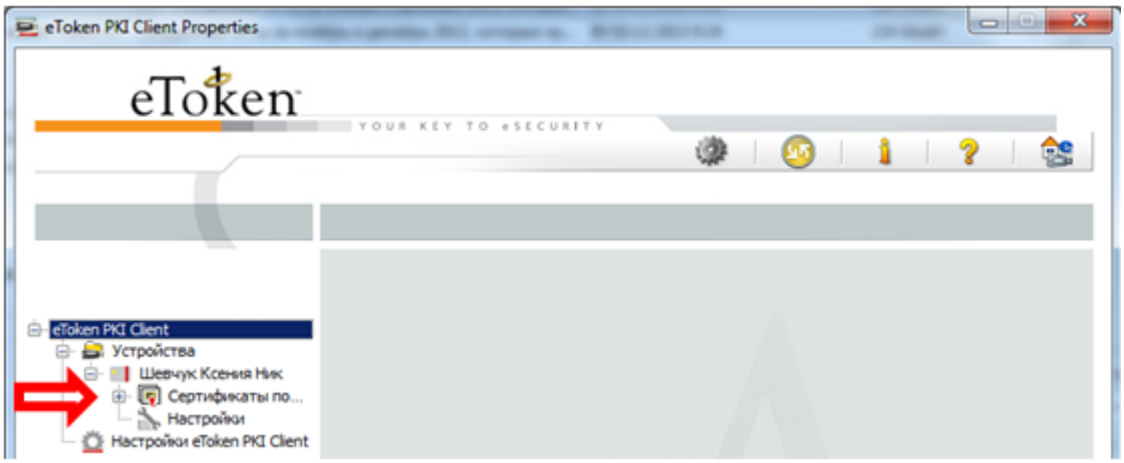


Рисунок 15. Просмотр имеющихся сертификатов на смарт-карте

- выбираем строку "Сертификаты пользователей" и просматриваем информацию об имеющихся на карте сертификатов. Нас интересует сертификат, выданный "CA-Samtg" и срок его действия (рисунок 16).

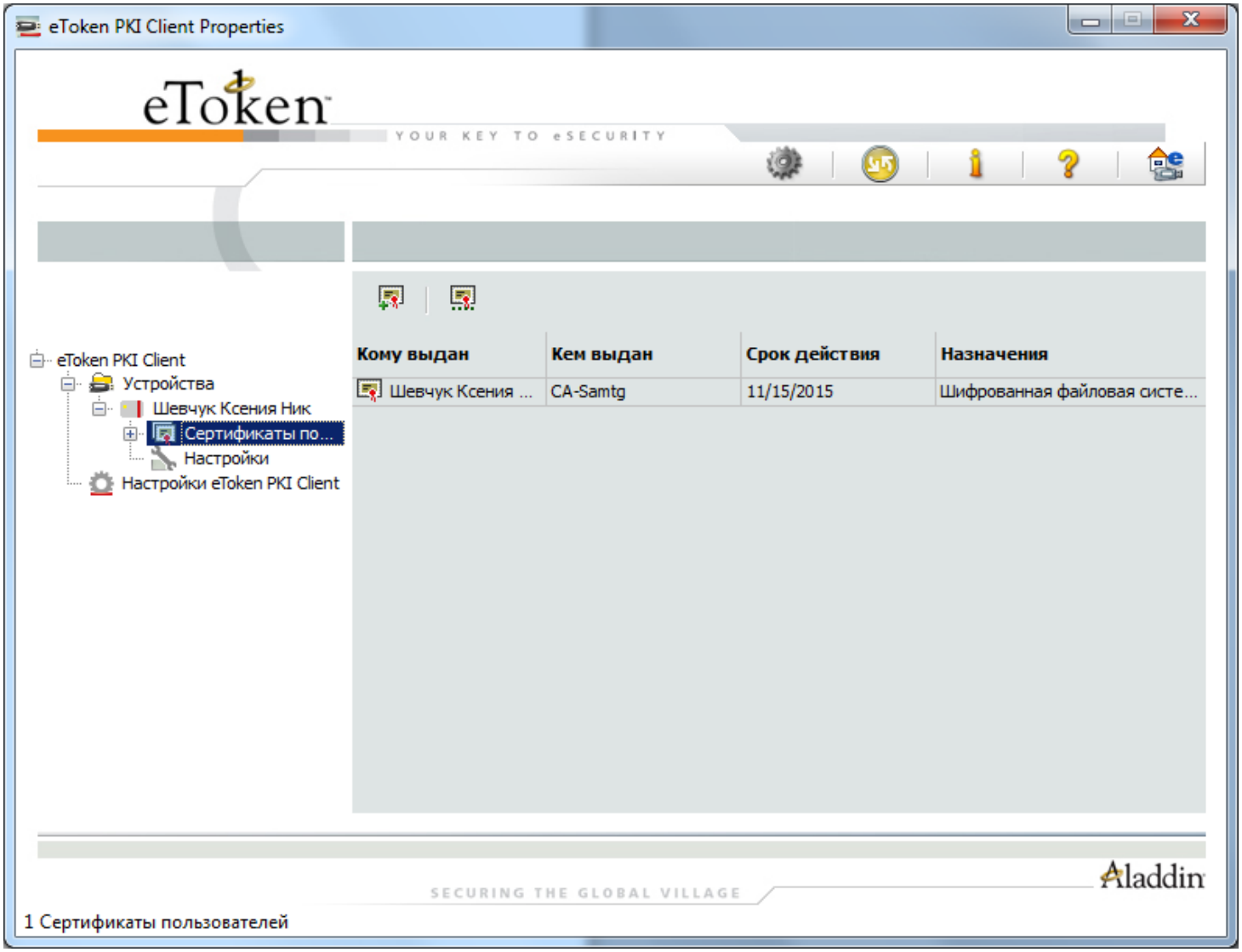


Рисунок 16. Просмотр срока действия выбранного сертификата

Если Срок действия сертификата истекает в ближайшие 7 дней, необходимо:

Обратиться в отдел поддержки пользователей - составив заявку через портал (рисунок 17).

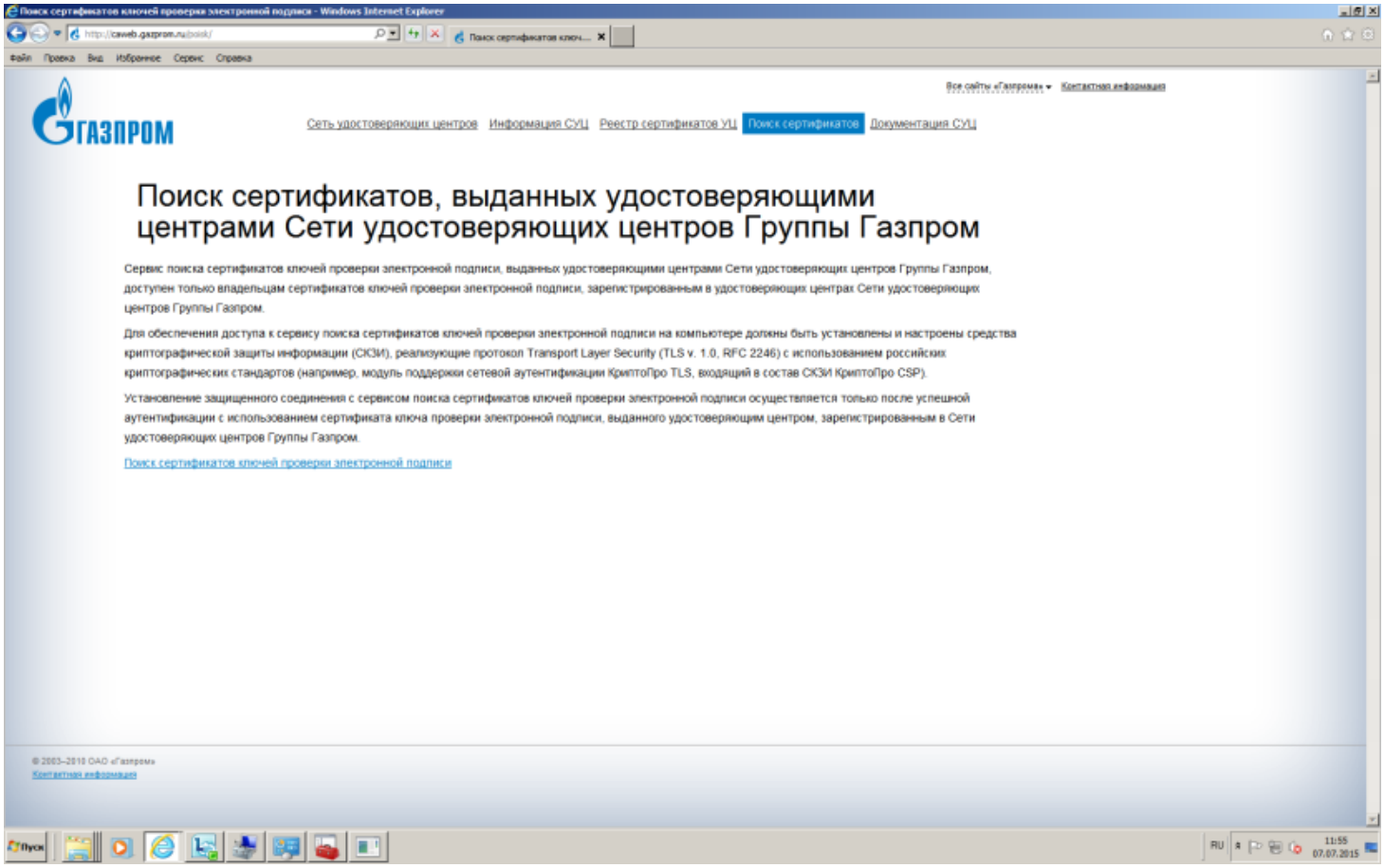


Рисунок 17. Обращение в отдел поддержки пользователей

Обработав Вашу заявку, специалист отдела поддержки пользователей (либо программист филиала) свяжется с вами и даст Вам инструкции, что делать дальше.

- подробные сведения о сертификате (рисунок 18).

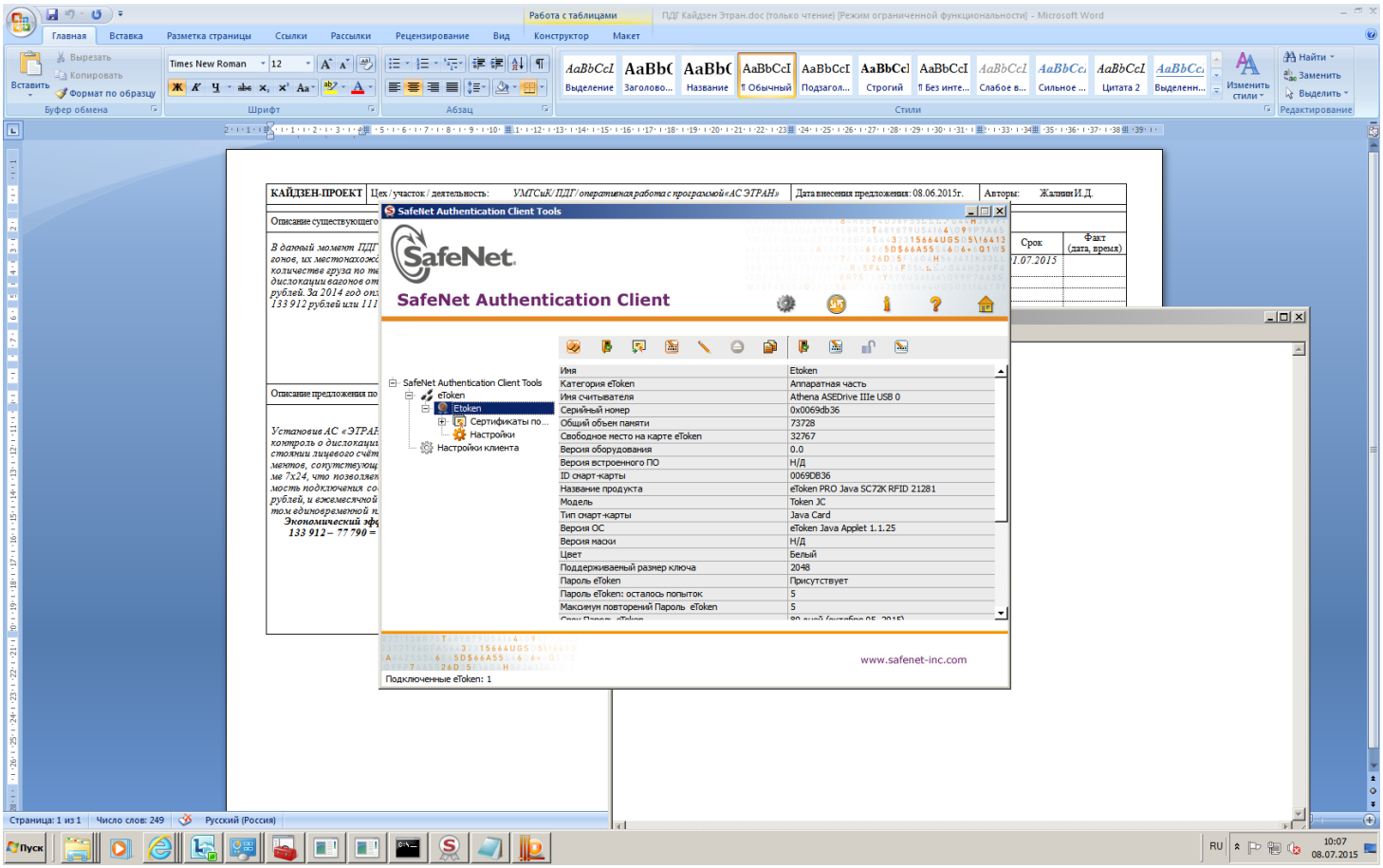


Рисунок 18. Просмотр сведений о сертификате

Проверка наличия сертификата и его срока действия для пользователя выполнена.

1. Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Информация, свободный. - Загл. с экрана. ↑

2. Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Информационная_безопасность, свободный. - Загл. с экрана. ↑

3. Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности, свободный. - Загл. с экрана. ↑

4. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2017. - 372 с. ↑

5. Спесивцев А.В. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков. - М. : Радио и связь, 2016. - 192 с. ↑

6. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М. : "ДМК пресс. Электронные книги", 2014. - 592 с. ↑

7. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. - М. : Академический проект, 2018. - 544 с. ↑

8. Семененко В.А. Информационная безопасность / В.А. Семененко. - М. : МГИУ, 2016. - 277 с. ↑

9. Мельников Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М. : Флинта, 2014. - 448 с. ↑

10. Конотопов М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М. : КноРус, 2014. - 136 с. ↑

11. Емельянова Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М. : Форум, 2015. - 368 с. ↑

12. Максименко В. Н. Защита информации в сетях сотовой подвижной связи / В.Н. Максименко, В.В. Афанасьев, Н.В. Волков. - М. : Горячая линия - Телеком, 2014. - 360 с. ↑

13. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М. : ГЛТ, 2018. - 558 с. ↑

14. Чипига А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М. : Гелиос АРВ, 2017. - 336 с. ↑

15. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. - СПб. : СПбГУ ИТМО, 2015. - 98 с. ↑

16. Урсул А. Д. Проблема информации в современной науке. - М. : Наука, 2017. ↑

17. Конотопов М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2016. - 136 с. ↑

18. Википедия - свободная энциклопедия [Электронный ресурс] / Режим доступа: https://ru.wikipedia.org/wiki/Криптография, свободный. - Загл. с экрана. ↑

19. Гришина Н. В. Аутентификация. Учебное пособие / Н.В. Гришина. - М. : Форум, 2015. - 240 с. ↑

20. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М. : Книжный мир, 2017. - 352 с. ↑

21. Емельянова Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М. : Форум, 2017. - 368 с. ↑

22. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах: моногр. / П.Н. Девянин. - М. : ИЛ, 2016. - 176 с. ↑