<эмблема-нормальная>

<**СТРОГО КОНФИДЕНЦИАЛЬНО**>
<**КОНФИДЕНЦИАЛЬНО**>
<ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ>
(ненужное удалить)

<логотип>

[данные-издателя]

Рег № [**СК**|**К**|**ОР**] Экз № из

dd.*mm*.200*y* № _____
СОГЛАСОВАНО
[Должность]
[Структурное подразделение]
_____ / И.О. Фамилия/
dd.*mm*.200*y*

УТВЕРЖДАЮ
[Должность руководителя]
[Краткое наименование предприятия]
_____ /И.О.Фамилия/
dd.*mm*.200*y*

Система защиты информации

УПРАВЛЕНИЕ КЛЮЧЕВЫМИ ДАННЫМИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММЫ ANETTO PASSWORD SAVER 1.5

КРАТКАЯ ИНСТРУКЦИЯ

Листов_____ за №№_____

РАЗРАБОТАНО
в соответствии с *руководством пользователя и опытом эксплуатации программы*.
[Должность]
[Структурное подразделение]
_____ / В.Н. Жаринов /
10.*06*.200*6*

г. <город-изд>

ВВЕДЕНИЕ В ДОКУМЕНТ

Общие положения

1. Файл содержит выполняемый автоматизированным способом (в форме машинного оригинала МО) [беловик|черновик] целевого документа или его части (неотъемлемой), выделенной для удобства работы.

Документ в целом, кроме основного содержания, может включать приложения. Содержание документа, приложения (его выделенной части) составляют текст и/или иллюстрации (графчасть).

Конкретное наполнение файла определяется по его имени (полный формат имён см. шаблон документа)[1].

2. Содержание документа, приложения подразделено на структурные элементы по иерархии; её верхние 4 уровня стандартны. Основная часть элементов имеет многоуровневую нумерацию и снабжена выделенными заголовками-абзацами, входящими в оглавление (описатель структуры элементов документа); имеются также элементы без нумерации, в т.ч. не входящие в оглавление, в т.ч. с заголовками в тексте (не выделенными как абзацы).

В тексте применяются типовые приёмы оформления, описанные в п/р 1.1 документа|шаблона.

3. В файл части из документа, приложения выделяется элемент структуры стандартного уровня иерархии (или ряд соседних элементов одного уровня) целиком (с заголовками).

Для многофайлового МО в имени каждого файла указаны индексы входящих элементов (формат: разделы <ЧN>, подразделы <пPNN>, пункты <ППNNN>, подпункты <пПNNNN>); файл первой части является *головным*.

При наличии приложений их форму (способ выполнения) указывают в отметках о наличии в составе единственного (или головного) файла основного документа (виды способов и формат отметок см. шаблон).

Приложения в МО могут выполняться как отдельные файлы *ПрилN* (что указывается в их отметках о наличии).

При наличии иллюстраций в документе, приложении (части) они также м.б. выполнены разными способами.

Иллюстрации в МО могут содержаться в отдельном от текста файле *Рисунки*; в этом случае текст содержится в файле *Текст* и в него для отсылки включаются подрисуночные подписи.

4. Оригинал документа (части) выполнен как настоящий файл (имя см. поле внизу) и другие необходимые (детальный состав многофайлового документа см. п. 1.1.4 в <настоящем файле|головном файле *Ч.1 Введ.*>).

Текст подготовлен в среде OpenOffice.org 2.4.0 Writer или иной программы, совместимой по файлам; иллюстрации выполнены в той же программе и/или иными средствами, включая захват машобразов для МО.

Подлинник выполняется как твёрдая копия с заменой и/или добавлением листов к твёрдой копии предыдущих версий, либо как электронный образ файлов оригинала по листам, с которого делаются твёрдые дубликаты.

5. Все права защищены их обладателями. Документ, а равно любая его часть в любой форме адресованы лицам, которые указаны автором как его адресаты и (или) третьим лицам, участвующим в совместной деятельности по соглашению между автором и указанными лицами; иное возможно только с письменного разрешения автора.

Документ предназначен для учебных, информационных, научных или культурных целей в соответствии с действующим законодательством РФ, включая, но не ограничиваясь, п.1 Ст.1274 ч.4 ГК РФ[2]. Содержание документа [используется «как есть»|м.б. изменено при совместной деятельности]. Пользователю разрешается: создать резервную копию каждого файла оригинала (при предоставлении только подлинника – каждого его листа) на случай утраты; делать одну твёрдую копию МО для правомерного пользования, включая замену утраченных (испорченных, потерянных) листов; цитировать документ в объёмах и порядке, разрешённых нормами авторского права РФ. Пользователь обязан: использовать оригинал (подлинник) и его копии (резервную и/или твёрдую) только лично и как указано выше; при цитировании документа ссылаться на источник[3]. Иное воспроизведение документа или любой его части в любой форме невозможно без письменного разрешения.

Информация, содержащаяся в документе, получена из открытых источников, рассматриваемых автором как надёжные. Возможное наличие секретных, конфиденциальных, а равно иных сведений ограниченного доступа следует рассматривать как результат предположения на массивах открытых сведений. Имея в виду возможные человеческие и технические ошибки, автор не может гарантировать абсолютную точность и полноту приводимых сведений, и не несёт ответственности за возможные последствия, связанные с их использованием.

Назначение, сведения о версиях, языковые соглашения

1. Документ содержит инструкцию для пользователей программы-менеджера паролей Anetto Password Saver 1.5 (далее – *программа*, *APS*).

[1] Переменные части текста даются как поля в '< >', заменяемые на описание; общая часть (корень) поля пишется как есть, а изменяемые части как '*'. Файлы МО с однокоренным именем относятся к одному элементу структуры.

[2] Федеральный закон № 230-ФЗ от 18 декабря 2006 г.

[3] Если цитата состоит полностью из сведений, цитирующих иной источник – сохраняя ссылку на первоисточник.

Программа может работать с информацией как личного, так и служебного характера. Чтобы использование программы для защиты служебной информации было правомерным, она должна быть допущена уполномоченными службами организации к применению как средство управления ключевыми данными. Решение о применении оформляется документально (приказом, распоряжением).

В инструкции предполагается, что программа используется для защиты информации, не составляющей государственную тайну, в негосударственной организации.

2. Версия документа определяется его датой и меняется при обновлении.

3. Термины, обозначения и сокращения данного документа введены в книгах /1/ и /2/, а также в Разделе 1. Также используются обозначения, описанные ниже.

Условные обозначения

1.1.1. В **тексте** документа применяются следующие приёмы оформления.

1.1.1.1. Чтобы ***упорядочить работу с материалом***, часть абзацев имеет особые стили.

Кроме обычного начала новой мысли с красной строки, наглядность повышается так:

- элементы перечисления удобно оформлять как пункты маркированного списка;

Без красной строки оформляются абзацы, отбиваемые в объёмном тексте мысли для удобства чтения (за первым), а также вводные положения к крупному элементу (под заголовком).

Формулы обычным текстом даются центрованно отдельных строках

> **Пример**. Такими абзацами выделяются примеры, иллюстрирующие текущую мысль основного текста. Так же выделяются практические рекомендации, советы, указания.
> – так в тексте примера выделяется пункт перечня;
> Так в тексте примера оформляется абзац продолжения текущей мысли.

Абзац с отступом и уменьшенным шрифтом выделяет в тексте документа составляющие развития, которые дополняют (уточняют, конкретизируют) содержание основного текста.

1.1.1.2. С той же целью фрагменты в тексте могут оформляться в следующих стилях:

Жирным шрифтом выделены названия отдельных пунктов, уровни классификации или комментарии в тексте к элементам схем, диаграмм.

Курсивом выделяются понятия, определяемые в тексте документа, а также предложения, содержащие важную информацию (выводы, указания и пр.). В списке литературы курсивом выделены позиции, которые имеются в [учебной|служебной] библиотеке.

Жирным курсивом выделены подуровни классификации либо понятия, о которых идёт речь в окружающем тексте, или которые уже должны быть Вам известны.

Подчёркиванием обозначаются сылки на место в данном документе или за его пределами, напр., на другие документы (кроме гиперссылок на ресурсы интернет, которые оформляются стандартно для эледоков). Если подчеркнута ссылка на другие дисциплины, сферы деятельности, то Вы можете обратиться за информацией к соответствующим специалистам, преподавателям, в интернет.

Разрядкой выделены места, на которые следует обратить особое внимание.

Таким начертанием (гарнитурой) шрифта и курсивом выделены наименования объектов (сущностей), описываемых в документе.

Такой гарнитурой шрифта (с уплотнением) выделены тексты процессов (алгоритмов, программ).

Такой гарнитурой шрифта выделены тексты указателей адреса сущностей (данных).

1.1.2. В **графической части** документа используются стандартные стили текста и условные обозначения, приведённые далее (см.[п. 1.3.2|Приложение<N>]).[Они идентичны тем, которые используются в [других документах, предметных областях]].

Так оформляется подрисуночная подпись

В файле выделенного текста эти подписи указывают наличие и положение иллюстраций.

> **Внимание**: отдельные подписи могут размещаться не под, а над рисунком. В любом случае подпись относится к тому рисунку, к краю которого она расположена вплотную.

Для иллюстрации того, о чем говорится в данный момент, приводятся конкретные примеры. Они оформляются так:

Пример. [содержание]

Так же выделяются практические рекомендации, советы, указания.

А так обозначены моменты, на которые Вам следует обратить особое внимание:

[***информация об узловом моменте текущего пункта или наиболее важных выводах их него***]

Или:

ВНИМАНИЕ: [***особое указание, требование, необходимое условие для применения пункта***]

Эта информация дается сразу же после того места в тексте, к которому она относится (как это сделано выше).

Оглавление

1. ВВЕДЕНИЕ

ВНИМАНИЕ: ***хорошо изучите этот раздел, чтобы ориентироваться в документе***.

1.1. Общие положения

1.1.1. В данной инструкции описано применение программы APS при управлении ключевыми данными (УКД) системы защиты информации (СЗИ), не составляющей государственную тайну.

1.1.2. Инструкция введена в действие [указать вид нормативного документа, его дату и номер].

В инструкции предполагается, что при защите любой информации действуют две категории режима: общий и особый.

Документ предназначен для [перечень должностей сотрудников] и может использоваться для сведения сотрудников [перечень взаимодействующих подразделений, организаций].

ВНИМАНИЕ: ***На момент использования Вами могут существовать законодательные ограничения в зависимости от возможностей используемой версии и предполагаемых условий применения. В частности, программа может подпадать под требования действующего законодательства о лицензировании основных видов деятельности по обеспечению её жизненного цикла, исходя из длины ключа и типа криптоалгоритма. См. также Положения, утверждённые ППРФ957-07 (перечень см. в*** Разделе 4***). Прежде, чем получить откуда-либо установочный комплект программы и использовать его, изучите действующие нормативные акты самостоятельно либо проконсультируйтесь с юристом.***

Потенциальная длина ключа APS составляет 64 бит (см. в п. 2.1.3***), а реальная длина ключа 27 бит обеспечивается только средствами программного контроля ввода ключа оператором. При наличии возможности редактировать файлы программы для ИТ-квалифицированного лица технически возможно отключить этот контроль, после чего реализуется потенциальная (или близкая к ней, если системно недопустимы отдельные символы для ввода) длина ключа. В связи с этим может измениться правовой статус программы как шифровального средства. Во избежание возможных в этом случае юридических претензий при эксплуатации программы вне нормативно регулируемых систем ЗИ в РФ следует обеспечить замкнутую программно-аппаратную (вычислительную) среду с целью исключения возможности вмешательства в программные файлы.***

1.1.3. Раздел 1 содержит сведения об управлении ключевыми данными как функции СЗИ.

В разделе 2 дана общая характеристика программы APS и описана процедура её установки.

Раздел 3 содержит описание применения APS в типичных ситуациях.

1.1.4. Документ подготовлен с использованием источников информации, указанных в разделе 4.

1.1.5. Основное содержание документа в оригинале выполнено как настоящий файл.

1.2. Понятие об управлении ключевыми данными

1.2.1. Ключевые данные (КД) используются для обеспечения информационной безопасности (ИБ) автоматизированных систем (АС) путем аутентификации пользователей (пароли) и криптографического преобразования информации (ключи шифрования). Механизмы, основанные на КД (шифрсистемы и парольные механизмы) являются основой технико-математической (ТМ) ЗИ.

1.2.2. К задачам управления ключевыми данными (УКД) относятся:

- Генерация ключей, паролей с характеристиками, затрудняющими их подбор (должны иметь достаточную длину, использовать широкий набор знаков, взятых в возможно более случайных сочетаниях).
- Распределение ключей, защищающих информацию при обмене, т.е. их передача от отправителей к получателям.
- Хранение ключей у пользователей и извлечение их по мере надобности.

К системам УКД предъявляются следующие требования:

- Распределение ключей возможно более удобным для пользователей, но не для потенциальных нарушителей образом.
- Удобство управления ключевыми данными (генерации, хранения и извлечения) для конкретного пользователя и организации группового использования ключей.
- Исключение *компрометации* КД, т.е. ознакомления с ними третьих лиц (среди которых могут быть реальные и потенциальные нарушители).

1.2.3. Как и в случае информационной деятельности, при практической реализации СЗИ существует различие в зависимости от класса процессов: местного хранения/обработки данных или обмена ими.

1.2.4. Для организации обмена отправителю и получателю необходимо заранее договориться о получении ключей на каждый сеанс обмена (сеансовых ключей).

Чтобы повысить защищенность ключевых данных и охраняемой информации от НСД, при конфиденциальном обмене необходимо следовать определённым организационным принципам. Они выработаны еще при обмене конфиденциальной информацией в натуральной форме.

Во-первых, ключи следует передавать от отправителя к получателю так, чтобы избежать их компрометации. Поэтому для передачи ключевых данных используется свой канал, отличающийся повышенной скрытностью от третьих лиц (принцип отдельного ключевого канала). Особенно это касается передачи ключей (паролей) в открытом виде (что хотя бы иногда неизбежно, если не используется шифрование самих КД с открытым ключом).

Для повышения надёжности в случаях, когда предполагается передача данных в открытом виде, используется шифрование с открытым ключом.

Во-вторых, необходимо учитывать возможность лобовой атаки на шифр или парольный механизм с использованием перехвата шифрованных сообщений и специальных средств анализа. Для повышения стойкости в этом случае следует использовать каждый сеансовый ключ только один раз (т.н. принцип минимального времени жизни ключей), причём генерировать ключи случайным образом, чтобы по ряду перехваченных ключей нельзя было предсказать следующие.

Чтобы сократить частоту пользования ключевым каналом, можно передавать ключи получателю не поодиночке, а заранее определённым списком (т.н. принцип шифроблокнота). Стороны могут заранее определить порядок выбора ключа из списка на каждый сеанс, чтобы дополнительно затруднить подбор ключей, если часть списка неожиданно станет известна третьим лицам. Однако это требует повышенной надёжности канала (в который в данном случае включаются и места хранения списка до его исчерпания), т.к. последствия компрометации потенциально усиливаются с увеличением числа ключей в списке.

Список сеансовых ключей для повышения защищенности следует передавать в зашифрованном виде. Разумеется, ключ к списку отправитель заранее должен передать получателю, но т.к. это делается редко, то вероятность компрометации ключей снижается.

В-третьих, для повышения стойкости обмена следует ограничить область разового доступа нарушителя. С этой целью часто применяется принцип вертикального разделения ключей. При этом сеансовый ключ используется для закрытия не самой передаваемой информации, а сообщения, содержащего ключ к передаваемому массиву. Можно ввести также горизонтальное разделение ключей, когда в одном сеансе передаются два и более массива, предварительно закрытые каждый своим ключом (паролем). В этом случае сеансовым ключом закрывается набор ключей к передаваемым массивам. Массивы подразделяются обычно по технологическим операциям, в которых они используются.

Шифрованный ключ (набор ключей) передаётся по ключевому каналу до начала использования первого из переданных в сеансе массивов. Очевидно, что задачи нарушителя в условиях разделения усложняются: при вертикальном нужно вскрывать шифр дважды, а при горизонтальном – также находить соответствие между ключами и массивами.

Для минимизации вероятности НСД также необходимо, чтобы нарушитель не мог одновременно получить и защищенные массивы, и таблицу ключей к ним. Поэтому массивы и ключи передаются по разным каналам (носителям), исходя из первого принципа.

1.2.5. В случае обработки/хранения проблемы несколько проще, т.к. обмен данными только внутри сосредоточенного КСА. Поэтому первый принцип видоизменяется в принцип отдельного ключевого носителя: ключевые данные хранятся отдельно от защищаемых (лучше всего на особом сменном носителе) и вводятся в КСА только для доступа к конкретному массиву ОхрД.

Второй принцип при сосредоточенной обработке состоит в периодической смене паролей доступа и шифров хранения. Для определения периода следует получить с помощью квалифицированных специалистов оценку минимального времени завершения перебора для каждого используемого механизма (шифрсистемы, парольного механизма) в зависимости от заданных возможностей нарушителя (вычислительные мощности и используемые средства реализации). Для минимизации вероятности НСД в этом случае необходимо менять ключи, пароли с интервалом, меньшим этого времени, а также защищать посредством конкретного механизма только информацию с временем жизни, меньшим оценочного.

Третий принцип в сосредоточенной системе реализуется при помощи спецсредств опознания и разграничения доступа к информации (ОРДИ) и контроля вычислительной среды (КВС). Средства ОРДИ реализуют регулярное горизонтально-вертикальное разделение доступа к ОхрД в пределах КСА и регламентируют действия любого пользователя и вычислительного процесса. Средства КВС следят за замкнутостью среды, в которой выполняются все задачи, в т.ч. специальные. Главная их задача – обнаружение несанкционированных изменений ресурсов любого ВПр (аппаратуры и ПО) и хода процесса, а также определение источника изменений (подмена конкретного оборудования и/или программ, атака извне системы) или хотя бы предоставление квалифицированному лицу максимума данных для обнаружения изменений и действий по ним.

1.2.6. Весь комплекс задач достаточно надёжно решается специальными программно-аппаратными средствами, с использованием шифрования ключей и специализированных носителей ключевых данных (НКД) типа карты памяти, Touch memory и пр. Однако эти решения дороги и применяются только в особо важных случаях.

1.2.7. Другой путь – чисто программная реализация функций УКД на обычных АРМ. В настоящее время для систем ИБ АС широкого применения удовлетворительно решена только первая задача путем использования программ-генераторов ключей. Для решения остальных традиционно используется либо запоминание текущих ключевых установок, либо запись их в открытом виде и помещение в какое-либо «укромное» место. Уже при нескольких ключах, па-

ролях на пользователя это становится неудобно и рискованно с точки зрения компрометации ключей.

Некоторые специализированные программы, например PGP, имеют встроенные механизмы управления ключами шифрсвязи, однако набор ключевых данных реального пользователя этим не ограничивается. Более того, в СЗИ при не слишком высоких требованиях к ИБ в первую очередь используется как раз не шифрсвязь, а другие механизмы защиты (парольного доступа к данным и ресурсам при обработке, закрытия хранимых файлов), которые часто не имеют необходимых средств управления ключевыми данными. Поэтому для комплексного решения задач УКД получили распространение отдельные программы – менеджеры.

1.3. Необходимые определения (для сложных и методических документов)

Здесь даются определения для терминов и обозначений, широко используемых в документе.

1.3.1. Терминология

Основные термины документа введены ранее в п/р 1.2.

1.3.2. Условные обозначения

Кроме описанных во введении в документ, используются специальные обозначения:

Обозначение	Наименование, краткая характеристика
Текстовые обозначения	
[описание части]	***Квадратные скобки*** в тексте документа выделяют переменную (в т.ч. необязательную) часть (вариант текста, параметр). На их место вводится информация, описанная внутри скобок или в указаниях, которые даются ниже (под соответствующим абзацем).
{описание части}	***Фигурные скобки*** в тексте документа выделяют необязательную часть.
XXX NN DDMM[YYYY/YY]	***Алфавитные шаблоны*** обозначают соответственно: • любой текст (такой же длины, как шаблон); • любое число (такой же длины); • место для даты (день, месяц, год полностью/сокращённо).
…	***Троеточие*** означает: • в цитатах – места разрыва цитирования; • в указаниях к.-л. диапазонов имеет смысл «от и до»; • в остальном тексте – указание на пропуск повторяющихся фрагментов.
< обозначение[, обозначение2, … обозначение N] >	В ***угловые скобки*** заключаются: • в тексте – обозначения клавиш и других органов управления, а также различных параметров; • в формулах – список (кортеж) констант и переменных. При нескольких параметрах (обычно 2…9) кортеж называют «парой», «тройкой», «четверкой» и т.д.
Действие | Действие |…	Через ***вертикальную черту*** в тексте указывается порядок действий в программных меню.

Обозначение	Наименование, краткая характеристика
Значение1/значение2/…	Через ***знак дроби*** (косая черта, англ. slash) в тексте слитно указывают возможные варианты, значения к.-л. показателя
Специальные текстовые выражения для алгоритмов, программ и машинных сообщений	
абв*	***Звездочка*** на конце текста означает, что эту и все оставшиеся позиции в тексте (до пробела) могут занимать любые символы (в т.ч. их вообще может не быть). **Пример.** При вводе текста oper* в качестве параметра запроса на поиск файлов будут найдены все файлы, имя которых начинается с oper, а от 0 до 4-х (в DOS) либо до 28-ми (в Windows) следующих символов будут любыми.
абв?где	***Знак вопроса*** внутри текста означает, что соответствующую позицию в тексте может занимать любой символ. **Пример.** При вводе текста oper?? в качестве образца для поиска файла будут найдены все файлы, имя которых начинается с oper, а следующие 2 символа будут любыми.

1.3.3. Сокращения

В документе употребляются следующие сокращения:

англ.	английский;
букв.	буквально;
в т.ч.	в том числе;
док.	документ;
и т.д.	и так далее;
и т.п.	и тому подобное;
к.-л.	какой-либо;
напр.	например;
см.	смотри;
т.е.	то есть;
т. зр.	точка зрения;
т.о.	таким образом;
разд.	раздел (документа);
п/р	подраздел (документа);
п.	пункт (документа);
п/п	подпункт (документа);
ОС	операционная система;
ППРФ	Постановление Правительства Российской Федерации;

2. ОБЩЕЕ ОПИСАНИЕ

2.1. Характеристика программы APS

2.1.1. Программа служит для управления ключевыми данными доступа к охраняемым данным (ОхрД) и к средствам автоматизации обработки таких данных.

Программа предназначена для работы в среде ОС *Windows 95/98/Me/NT/2000*.

2.1.2. Основные функции программы APS:

- Ведение базы ключевых данных (в терминологии авторского руководства - *таблицы*) простейшего формата, содержащей значения ключевых данных и вспомогательные сведения;
- Криптографическая защита таблицы при её хранении в файле.

Каждый пользователь программы может создать одну или много таблиц и управлять каждой из них в отдельности. За счет сведения в таблицу большого числа паролей пользователь избавлен от необходимости запоминать их (или записывать «на манжетах» с риском раскрытия злоумышленниками) – нужно помнить лишь единственный пароль для каждой таблицы.

В комплект APS входит также отдельная утилита APS PGP, имеющая функции:

- Создание криптографически защищенного самораспаковывающегося архива (непрерывного или многотомного) из файлов, выбранных пользователем (в т.ч. из разных каталогов).
- Извлечение по ключу файлов из архива в папку, указанную пользователем.

2.1.3. Характеристики APS:

- Число строк в таблице: *не ограничено*.
- Число полей строки: *3 (логин, пароль, описание)*.
- Формат полей: *текстовые, произвольной длины* (длина видимой части фиксирована).
- Наличие открытых данных при хранении: *нет* (таблица в открытом виде существует только в ОП).
- Число файлов в архиве: *не ограничено*.
- Местоположение исходных файлов перед упаковкой: *произвольное* (выбор в поиско-вом окне).
- Размер тома многотомного закрытого архива: *250/420/1024/1440тыс.Б/1.44МБ* (по выбору пользователя).
- Местоположение закрытого архива: *по выбору пользователя* (через поисковое окно).
- Наличие открытых данных после упаковки: *да* (сохраняются исходные файлы).
- Используемый алгоритм: *PGP*.

ВНИМАНИЕ! ***Хотя автором APS указана длина ключа 64 бит (сравнительно малая по современным требованиям), фактически она искусственно уменьшена за счет того, что ключ логически состоит из 8 байт, для каждого из которых выбираются только двоичные кла-виатурные коды десятичных цифр (0…9). Т.о. всего возможно не 2^{64}~10^{19} различных ключей, а только 10^{8}~2^{27} (т.е. фактическая длина ключа составляет 27 бит).***

Хотя стойкость используемого в программе алгоритма PGP в данное время не вызывает сомнений, столь малая длина ключа позволяет потенциальному нарушителю при наличии доступа к значительным вычислительным мощностям «вскрыть» любой ключ APS путем прямого перебора ключей за время, меньшее времени жизни информации в закрытом массиве (таблице, архиве).

2.1.4. В данной инструкции рассмотрено использование программы для типичных задач управления ключевыми данными при защите служебной информации. За более подробной ин-

формацией по функциям APS обратитесь к авторскому руководству пользователя (файл *main.htm* в каталоге …\APS\Help\, далее - *Справка*).

Внимание! Если Вы также используете программу для управления личными ключами, паролями, категорически запрещается смешивать личные и служебные ключевые записи в одной таблице, а также вызывать личные таблицы для обработки в рабочее время!

2.2. Установка программы

2.2.1. Установочный комплект представляет собой приложение (файл *apssetup.exe*).

2.2.2. При запуске указанного файла выводится подготовительное сообщение, после чего раскрывается окно *Setup*.

2.2.3. Процесс установки включает стандартные для большинства программ шаги:

- Ознакомление с лицензионным соглашением;
- Запрос местоположения каталога для установки программы (папка *. . .* \APS);
- Выбор размещения программы в меню «Пуск» Windows.

ВНИМАНИЕ! ***Каталог программы должен находиться в отдельной папке, определённой для специальных программ. Не допускается установка APS в стандартный каталог приложений*** …\Program files.

2.2.4. После успешного завершения программа готова к использованию. Ошибки могут быть связаны с несоответствием версии ОС.

2.2.5. Основные функции APS кратко описаны в авторском руководстве. Далее рассмотрено решение при помощи программы конкретных задач управления ключевыми данными со ссылками на *Справку* (чтобы не дублировать содержащиеся там сведения).

3. ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ

3.1. Вызов и настройка

3.1.1. Первоначально программа вызывается из *меню «Пуск»* либо с *Рабочего стола* (если при установке была выбрана опция добавления значка APS на Рабочий стол).

3.1.2. При вызове программы появляется диалоговое окно «*Идентификация пользовате-ля*». В поле «*Вас зовут*» введите желаемое имя пользователя (фактически речь идёт об имени таблицы). Выпадающий список поля содержит уже существующие имена, из которых можно выбрать.

ВНИМАНИЕ! ***Если программа переустановлена в процессе использования, информация об именах созданных таблиц теряется (выпадающий список пуст).***

Если набранное имя неизвестно программе, она предлагает создать нового пользователя (т.е. завести пустую таблицу с заданным именем). Вы можете подтвердить это и ввести пароль (до 8 цифр) либо отказаться.

По умолчанию вновь созданная таблица имеет одну пустую запись.

Помимо открытия/создания таблиц Вы можете выбрать режим демонстрации кнопкой «*Взгляд*» или открыть *Справку* кнопкой «*Помощь*».

При вводе существующего имени и корректного пароля выбранная таблица считывается с ключевого носителя и расшифровывается, после чего доступна для работы.

3.1.3. В меню *Настройки,Внешний вид* установите желаемый вид интерфейса (см. Справка, разд. Настройки программы) и подтвердите ввод.

ВНИМАНИЕ! ***Необходимо включить опцию «Спрашивать пароль при выходе из трея» в разделе «Личные настройки».***

В данном меню Вы также можете выбирать один из двух режимов работы программы: «Дом» или «Офис» (Справка, разд. Настройки программы).

3.1.4. Чтобы изменить имя и/или пароль для открытой таблицы, войдите в меню *Настройки,Личные*, сделайте необходимые изменения в диалоговом окне (см. Справка) и подтвердите выбор кнопкой «*Да*».

ВНИМАНИЕ! ***Если Вы забыли пароль, доступ к таблице за приемлемое время практически не-возможен (исключая случай, описанный в*** п. 1.3.3***). Поэтому не заводите одновременно слишком много таблиц, иначе Вы встанете перед той же проблемой, которую хотели ре-шить применением APS.***

3.1.5. Большинство функций программы вызывается как через меню, так и кнопками на панели инструментов (описание см. Справка, разд. Основное окно), а также «горячими кла-вишами».

Все команды меню *Операции* также доступны в контекстном меню. Для вызова данного меню достаточно щёлкнуть на нужной строке правой кнопкой мыши (предварительно следует указать эту строку, щёлкнув на ней левой кнопкой). Далее выбирается нужная команда. При описании мы будем указывать вызов команд через контекстное меню, поскольку этот способ наиболее прост.

3.1.6. Для окончательного выхода из программы используется команда меню *Операции,Выйти* (недоступна из контекстного меню).

Программа также может быть добавлена в системную область *Панели задач Windows* (т.н. «*трей*») через команду меню *Операции,Свернуть в трей* (при этом появляется значок программы рядом с часами).

Программа вызывается из трея щелчком правой кнопки мыши на значке. Далее выполняется обычная процедура, как в п. 3.1.2.

При окончательном выходе APS убирается из трея и должна снова вызываться, как указано в п. 3.1.1.

ВНИМАНИЕ! ***Программа в трее работает только с текущей таблицей. Открыть новую таблицу можно только после окончательного выхода. В целях конспирации не рекомендуется слишком часто помещать APS в трей.***

3.2. Ключевые данные и работа с ними

3.2.1. Основные виды ключевых данных, необходимые пользователю АИС:

- Пароль на вход в базовую системную программу обслуживания (BIOS Setup).
- Пароль начальной загрузки компьютера (устанавливается в BIOS Setup).
- Пароль на вход пользователя в систему (устанавливается в ОС).
- Пароли доступа к прикладным программам.
- Пароли/ключи для доступа к защищенным файлам, папкам, областям внешней памяти (устанавливаются в ОС, прикладных программах, специальных средствах ЗИ).
- Ключи шифрования для конфиденциальной связи (если управление ими не встроено в соответствующие шифрсредства).

Необходимость ключей, паролей в каждом конкретном случае и режим их использования (общий или особый) определяется по согласованию с сотрудником, уполномоченным по ИБ в Вашем подразделении.

Если имеется уверенность в том, что нарушитель в состоянии применить прямой перебор ключей, следует получить с помощью квалифицированных специалистов оценку минимального времени завершения перебора (пример такой оценки см. в статье /2/***). Для минимизации вероятности НСД в этом случае необходимо менять ключи к таблицам APS с интервалом, меньшим этого времени, а также защищать посредством APS PGP только ОхрД с временем жизни, меньшим минимального.***

3.2.2. Пользователь в общем режиме ИБ ведёт одну таблицу для хранения всех служебных ключей. Программа может работать постоянно в режиме «Дом».

ВНИМАНИЕ! ***При создании/редактировании записей исключите возможность ознакомления посторонних лиц с информацией на экране. При использовании ключевых данных переводи-те программу в режим «Офис», если Вы не можете быть уверены в недоступности экрана для посторонних.***

В особом режиме пользователь ведёт отдельную таблицу для ключевых данных, используемых только в этом режиме. Программа устанавливается в режим «Дом» только на время создания/редактирования таблицы, при использовании ключевых данных программа должна работать в режиме «Офис».

ВНИМАНИЕ! ***Пароль и имя каждой таблицы следует запомнить. Нельзя записывать их где-либо во избежание компрометации всех ключей в таблице!***

3.2.3. Для создания записи о ключе, пароле:

3.2.3.1. Установите программу в режим «Дом» (если текущий режим «Офис»).

3.2.3.2. Щёлкните *правой* кнопкой где-либо на поле таблицы. В контекстном меню выберите команду «Добавить запись».

3.2.3.3. В появившемся диалоговом окне (Справка, разд. Добавление / Редактирование записи) введите в поле «*Логин*» имя пользователя, если оно требуется в программе, для которой предназначен ключ, пароль (далее – *программа-потребитель*).

Если имя пользователя не нужно, рекомендуется использовать поле «*Логин*» для указания назначения ключевых данных.

3.2.3.4. Введите задуманное значение ключа либо сгенерируйте значение кнопкой инструментов в поле окна «*Пароль*».

3.2.3.5. Составьте краткое описание, чтобы ориентироваться в назначении ключа, и введите его в поле «*Описание*».

ВНИМАНИЕ! ***Не рекомендуется вводить в поля «Логин» и «Пароль» информацию, не умещающуюся в видимую область поля. В этом случае для чтения всего поля придется перемещаться в нем при помощи курсора. Тогда считывание записи замедляется, и в режиме «Дом» более веро-ятно несанкционированное ознакомление с ней.***

3.2.3.6. Подтвердите ввод кнопкой «*Да*». Вы увидите в таблице новую ключевую запись (строку).

Повторяя эти действия, создайте все необходимые записи.

3.2.4. Вы можете изменять порядок следования строк в таблице, как Вам удобно. Для этого:

3.2.4.1. Установите программу в режим «Дом» (если текущий режим «Офис»).

3.2.4.2. Щёлкните *левой* кнопкой на строке, которую хотите передвинуть.

3.2.4.3. Убедившись, что курсор находится на одной из ячеек нужной строки, войдите в контекстное меню щелчком правой кнопки.

3.2.4.4. Выберите пункт Подвинуть запись вверх/вниз. Запись будет перемещена на одну позицию в указанном направлении.

Повторяйте эту последовательность действий с одной или разными строками, пока не добьетесь желаемого порядка записей в таблице.

3.2.5. Для редактирования записи:

3.2.5.1. Установите программу в режим «Дом» (если текущий режим «Офис»).

3.2.5.2. Щёлкните *левой* кнопкой на строке, которую хотите передвинуть.

3.2.5.3. Убедившись, что курсор находится на одной из ячеек нужной строки, войдите в контекстное меню щелчком *правой* кнопки.

3.2.5.4. Выберите пункт Редактировать запись. Появится диалоговое окно, как в п/п 3.2.3.2.

3.2.5.5. Переходите к нужному полю и редактируйте его.

3.2.5.6. Нажмите кнопку «*Да*» для сохранения результата.

3.2.6. Для использования ключа, пароля:

3.2.6.1. Откройте нужную таблицу, как указано в п. 3.1.2.

3.2.6.2. Щёлкните *левой* кнопкой на строке, которую хотите передвинуть.

3.2.6.3. Убедившись, что курсор находится на одной из ячеек нужной строки, войдите в контекстное меню щелчком правой кнопки.

3.2.6.4. В появившемся контекстном меню выберите команду «Скопировать», далее выберите «*Пароль*». Независимо от режима работы («Дом» или «Офис») в буфере обмена Windows окажется истинное значение пароля.

3.2.6.5. Перейдите к программе-потребителю и войдите в ней в режим ввода пароля.

3.2.6.6. Вставьте в соответствующее окно пароль из буфера (это делается щелчком *правой* кнопки мыши на окно, затем в появившемся контекстном меню выбирается команда «Вставить»). После входа в программу-потребитель закройте таблицу.

ВНИМАНИЕ! ***Некоторые потребители паролей не допускают возможности вставки значений из буфера. Тогда Вам придется вводить пароль, ключ вручную. Чтобы не выходить из режима «Офис», вызовите программу Блокнот (в англоязычной Windows - Notepad) и вставьте туда содержимое буфера (независимо от режима APS оно отобразится в истинном виде). Введите значение вручную, читая его из Блокнота.***

Немедленно после входа в программу-потребитель закройте Блокнот без сохранения!

3.2.7. Программа предоставляет возможность генерировать пароль в любой момент, а не только при создании ключевой записи. Для этого:

3.2.7.1. Вызовите генератор паролей через меню *Сервис*.

3.2.7.2. В появившемся диалоговом окне (Справка, разд. Генератор паролей) настройте параметры генерации в зависимости от допустимого формата пароля программы-потребителя.

3.2.7.3. Нажмите кнопку «Сгенерировать», а затем кнопку «Скопировать». Закройте генератор.

3.2.7.4. Вызовите программу, для которой предназначен пароль, и войдите в ней в режим ввода пароля.

3.2.7.5. Вставьте в соответствующее окно пароль из буфера (см. п. 3.2.6).

Чтобы выйти из генератора паролей, не выполнив никаких действий, щёлкните кнопку закрытия окна «*X*».

3.3. Обмен данными с использованием программы

3.3.1. Программу можно использовать при обмене защищенными массивами данных (файлами) между удалёнными рабочими местами (если для передачи соответствующих массивов не определено специальное средство конфиденциальной связи).

Далее предполагается, что конфиденциальная связь организуется на принципах отдельного ключевого канала, шифроблокнота и горизонтального разделения ключей.

3.3.2. Для организации обмена отправителю и получателю необходимо заранее договориться о получении ключей на каждый сеанс обмена (сеансовых ключей).

ВНИМАНИЕ! ***В силу небольшой фактической длины ключа APS (см. выше в п. 1.3.3) нужно соблюдать конфиденциальность связи. Способ и факт передачи ключей в открытом виде следует надёжно скрывать от третьих лиц. То же относится и к передаче шифрованной информации.***

Список сеансовых ключей для передачи можно оформить как ключевую таблицу, а можно в виде файла, защищаемого утилитой *APS PGP*. Эту же утилиту можно применить и для защиты передаваемых массивов данных (если для этого уже не определено другое средство).

Ключи хранятся, как указано в п. 3.4.4.

Очередной сеанс передачи конфиденциальной информации осуществляется при наличии ключа на этот сеанс.

3.3.3. Для передачи конфиденциальной информации в текущем сеансе отправителю необходимо:

3.3.3.1. Создать временную таблицу, как указано в п. 3.1.3, используя в качестве пароля очередной сеансовый ключ.

3.3.3.2. Заполнить её ключами по числу одновременно передаваемых в данный адрес массивов данных (закрытых архивов), как указано в п. 3.2.3. Имя и описание ключа должно позволить получателю однозначно выбрать нужный ключ для каждого массива.

3.3.3.3. Защитить последовательно каждый отправляемый массив (файл, папку) так, как это предусмотрено (шифрованием, паролем доступа). Каждый раз ключ передаётся из соответствующей строки таблицы через буфер обмена (кнопка «*страничка*» меню записи).

3.3.3.4. Записать отправляемые массивы на носители данных, после чего уничтожить ненужные исходные файлы.

3.3.3.5. Экспортировать временную таблицу на ключевой носитель, как указано далее в п. 3.4.2.

3.3.3.6. Отправить массивы и временную таблицу по отдельным каналам обмена (на сменных носителях или по сети).

ВНИМАНИЕ! ***При работе с информацией в особом режиме запрещается одновременная передача временной таблицы и защищенных массивов по общему каналу обмена. Это связано с низкой стойкостью ключей APS, как и APS PGP (см. выше в*** п. 1.3.3***).***

3.3.4. Получателю конфиденциальной информации необходимо:

3.3.4.1. Импортировать временную таблицу на своем рабочем месте, как указано далее в п. 3.4.3.

3.3.4.2. По мере необходимости открывая таблицу, определять содержание каждого массива по описаниям и извлекать нужные ключи, пароли.

3.3.4.3. Передавать ключ, пароль в соответствующую программу и выполнять доступ к нужному массиву.

Далее массив обрабатывается согласно технологии.

По завершении передачи всех массивов временная таблица уничтожается.

3.4. Обращение носителей ключевых данных

3.4.1. По умолчанию для каждой таблицы отводится своя папка в каталоге программы APS (имя этой папки совпадает с заданным в поле «*Вас зовут*»). Иначе говоря, в качестве носителя ключевых данных используется каталог на устройстве внешней памяти, куда Вы установили программу (обычно на Вашем жёстком диске).

Если Вам необходимо получать таблицы извне и передавать их на другие НКД (например, на дискетах или по сети), пользуйтесь функциями импорта/экспорта паролей (их описание см. Справка, разд. Импорт/Экспорт таблиц паролей).

При экспорте таблица дублируется в отдельную папку-источник за пределами каталога программы (в т.ч. на ключевой дискете или удалённом компьютере). Программа по-прежнему работает с таблицами, чьи папки находятся в её каталоге, а папки-источники не используются.

После импорта программа APS получает доступ к содержимому сохранённой таблицы (на том же компьютере или на любом, куда скопирована папка-источник).

3.4.2. Для экспорта таблицы, т.е. записи в папку-источник:

3.4.2.1. Откройте или создайте таблицу, которая будет переноситься.

3.4.2.2. Если нужно экспортировать на дисковод, вставьте нужную ключевую диске-ту.

3.4.2.3. Выберите в меню Операции,Экспорт.

3.4.2.4. В появившемся диалоговом окне (см. Справка, разд. Импорт/Экспорт таблиц паролей) укажите путь для экспорта (дисковод или каталог). Если там нет папки для таблицы, нажмите кнопку создания и введите имя папки в следующем диалоговом окне. В строке состояния должно быть «*Готов для экспорта*».

3.4.2.5. Подтвердите операцию кнопкой «*Да*». После выполнения появится сообщение о результатах.

После успешного экспорта* НЕМЕДЛЕННО *удалите папку с соответствующим именем из каталога программы.

3.4.3. Для импорта таблицы, т.е. считывания из папки-источника:

3.4.3.1. Войдите в APS с именем и паролем желаемой таблицы. Если такой таблицы еще нет, то в каталоге APS появится папка для неё.

3.4.3.2. Если нужно импортировать с дисковода, установите туда нужную ключевую дискету.

3.4.3.3. Выберите в меню Операции,Импорт.

3.4.3.4. В появившемся диалоговом окне (Справка, разд. Импорт/Экспорт таблиц паролей) укажите путь к папке желаемой таблицы (на жёстком диске или дисководе). В строке состояния должно быть «*Готов для импорта*».

3.4.3.5. Подтвердите операцию кнопкой «*Да*». После выполнения появится сообщение о результатах. Одновременно информация из таблицы-источника заместит текущую.

После импорта папка-источник очищается и таблица становится недоступна для импорта. Если требуется возможность многократного импорта, папку-источник нужно заранее продублировать. Целесообразно заархивировать папку, поместив архив рядом с ней.

3.4.4. Ключевые дискеты учитываются, хранятся, выдаются в соответствии с порядком обращения конфиденциальных машинных носителей для соответствующего режима ИБ.

Запрещается запись на один сменный носитель либо в один каталог на фиксированном носителе охраняемой (служебной) информации и ключевых данных.

Ключевые дискеты хранятся отдельно от носителей служебной информации (выделенные сейфы, ячейки).

Если в число принятых угроз входит пожарная опасность, для хранения используются сейфы, отвечающие специальным требованиям по огнестойкости (выбираются по рекомендациям уполномоченных организаций).

В особом режиме таблица после создания/редактирования либо использования* НЕМЕДЛЕННО *переносится на сменный ключевой носитель, как указано в* п. 3.4.2*.

4. ИСТОЧНИКИ ИНФОРМАЦИИ

Документы для ссылок

1. Лицензирование деятельности, связанной с информацией и её защитой. – М.: «Книга сервис», 2003.
2. Пудовченко Ю. Когда наступит время подбирать ключи.//Конфидент-ЗИ.

Нормативные акты

В качестве индекса нормативного акта используется его аббревиатура (номер) и год издания. Для нормативных документов, утверждённых другими документами, спереди через дробь добавляется индекс утверждающего акта (закона, постановления, указа, распоряжения).

ППРФ957-07. «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» от 29 декабря 2007 г. №957.

ПоЛРШС. «О лицензировании деятельности по распространению шифровальных (криптографических) средств» (утверждено ППРФ957-07).

ПоЛТОШС. «О лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств» (утверждено ППРФ957-07).

ПоЛПУШИ. «О лицензировании деятельности по предоставлению услуг в области шифрования информации» (утверждено ППРФ957-07).

ПоЛРПШС. «О лицензировании деятельности по разработке, производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем» (утверждено ППРФ957-07).

ПРИЛОЖЕНИЯ

1. [Заголовок приложения] [указание формы документа: оригинал/дубликат/машинная копия/файл)] [указание файла машинного документа]).

> **Внимание**: Данный перечень составляется для приложений, выполненных отдельно и не включённых в содержание документа. Указание файла возможно разными способами (см. п. 3.4.6 шаблона).

[Краткое наименование документа] разработан в соответствии с *[указать причину или документ, послуживший основанием для создания документа]*.

[Должность, структурное подразделение] _____ / И.О. Фамилия /
dd.*mm*.200*y*

СОГЛАСОВАНО

[Должность 1]
[Организация, структурное подразделение 1] _____ / И.О. Фамилия /
dd.*mm*.200*y*
…
[Должность N]
[Организация, структурное подразделение N] _____ / И.О. Фамилия /
dd.*mm*.200*y*

Исп. [Фамилия И.О.], тел. [{код }номер]

ЛИСТ ОЗНАКОМЛЕНИЯ

С [Наименование документа] ознакомлен _____ /И.О.Фамилия/
dd.*mm*.200*y*

С [Наименование документа] ознакомлен _____ /И.О.Фамилия/
dd.*mm*.200*y*

С [Наименование документа] ознакомлен _____ /И.О.Фамилия/
dd.*mm*.200*y*

Внимание: Данный лист необходим только для документов нормативного характера.