

	<p align="center">ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014</p>	<p align="center">Издание 2014-09</p>
		<p align="center">Лист 2 из 16</p>

Содержание

1 Назначение.....	3
2 Область применения.....	3
3 Нормативные ссылки.....	3
4 Обозначения и сокращения.....	3
5 Организация работ.....	4
5.1 Общие требования.....	4
5.2 Учет, хранение СКЗИ и криптографических ключей.....	6
5.3 Размещение, охрана и организация режима в помещениях, где установлены СКЗИ	8
5.4 Контроль за организацией, обеспечением функционирования и безопасности СКЗИ	9
6. Внесение изменений.....	9
7. Рассылка.....	9
8. Приложения.....	9
Лист регистрации изменений.....	14
Лист ознакомления.....	15
Лист рассылки.....	16

НЕУЧТЕН

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 3 из 16
---	---	-------------------------------------

1 Назначение

Настоящая инструкция определяет порядок учета, хранения и использования средств криптографической защиты конфиденциальной информации (СКЗИ) и криптографических ключей, в целях обеспечения безопасности эксплуатации СКЗИ в ФГБОУ ВПО Самарская ГСХА.

2 Область применения

Требования данной инструкции распространяются на пользователей средств криптографической защиты информации ФГБОУ ВПО Самарская ГСХА, участвующих в организации и обеспечении безопасности эксплуатации шифровальных (криптографических) средств в информационной системе.

3 Нормативные ссылки

Данная инструкция разработана с учетом требований следующих правовых и нормативных документов:

- Федеральный закон Российской Федерации от «27» июля 2006 г. № 152-ФЗ «О персональных данных»;
- Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 N 28608);
- Постановление Правительства РФ от «01» ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Положение по аттестации объектов информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г.;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), Гостехкомиссия России, 2002 г.;
- РД «Концепция защиты СВТ и АС от НСД к информации», Гостехкомиссия России, 1992 г.;
- РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1992 г.
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 № 149/6/6-622)
- СМК 02-09-2013 Документированная процедура системы менеджмента качества. Общие требования к содержанию и оформлению положений о деятельности;

4 Обозначения и сокращения

В настоящей инструкции использованы следующие сокращения и обозначения:

- **ФГБОУ ВПО Самарская ГСХА или академия** – федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарская государственная сельскохозяйственная академия»;

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 4 из 16
---	---	-------------------------------------

- **РФ** – Российская Федерация;
- **РД** – руководящий документ;
- **ФСТЭК** - Федеральная служба по техническому и экспортному контролю;
- **СВТ** – средства вычислительной техники;
- **НСД** – несанкционированный доступ;
- **ответственный пользователь СКЗИ** – это пользователь, который отвечает за безопасность средств криптографической защиты информации;
- **ПЭВМ** – персональная электронно-вычислительная машина;
- **ФСБ** – федеральная служба безопасности;
- **СМК** – система менеджмента качества;
- **Компрометация** - факт доступа постороннего лица к защищаемой информации, а также подозрение на него;
- **Криптосредства** – шифровальные (криптографические) средства;
- **СКЗИ** - сертифицированные федеральной службой безопасности (Федеральное агентство правительственной связи и информации при Президенте Российской Федерации) средства криптографической защиты конфиденциальной информации;
- **Криптоключ** – криптографический ключ;

5 Организация работ

5.1 Общие требования

5.1.1 Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами, приказом ректора ФГБОУ ВПО Самарская ГСХА назначается ответственный пользователь СКЗИ (далее – ответственный пользователь СКЗИ).

5.1.1.1 Ответственный пользователь СКЗИ выполняет следующие функции:

- определяет необходимость использования СКЗИ для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;
- устанавливает и вводит в эксплуатацию криптосредства в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверяет готовность криптосредств к использованию с составлением заключений о возможности их эксплуатации;
- обучает пользователей СКЗИ, использующих криптосредства, работе с ними;
- ведет поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним, носителей персональных данных;
- ведет учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);
- осуществляет контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;
- составляет заключение по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 5 из 16
--	---	-------------------------------------

снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5.1.1.2 Ответственный пользователь СКЗИ имеет право:

- требовать соблюдения инструкций, требований эксплуатационной и технической документации к СКЗИ;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования СКЗИ;
- участвовать в анализе ситуаций, касающихся функционирования СКЗИ и расследования фактов несанкционированного доступа.

5.1.1.3 Ответственный пользователь СКЗИ обязан:

- обеспечивать функционирование и поддерживать работоспособность СКЗИ в пределах возложенных функций;
- вести поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;
- сообщать руководству о неправомерных действиях пользователей СКЗИ, приводящих к инцидентам информационной безопасности (нарушения целостности, доступности и конфиденциальности информации);
- обеспечить выполнение требований нормативных документов по порядку хранения действующих криптосредств, резервных СКЗИ, эксплуатационной и технической документации к ним.

- вести документацию в соответствии с требованиями нормативных документов.

5.1.1.4 Ответственный пользователь СКЗИ несет ответственность:

- за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией - в пределах, определенных действующим законодательством Российской Федерации;
- за правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.1.2 Пользователи СКЗИ назначаются приказом ректора ФГБОУ ВПО Самарская ГСХА.

Пользователь СКЗИ обязан:

- строго соблюдать правила пользования СКЗИ и требования настоящей инструкции;
- не допускать установки на ПЭВМ нештатных программ, предупреждать возможность занесения вирусов и других вредоносных программ;
- не разглашать информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 6 из 16
--	---	-------------------------------------

- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов в другие ПЭВМ.

5.1.3 Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на ответственного пользователя СКЗИ.

5.1.4. Ответственный пользователь СКЗИ и пользователи СКЗИ должны быть ознакомлены с типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными ФСБ России от 21 февраля 2008 г. № 149 и настоящей инструкцией.

5.2 Учет, хранение СКЗИ и криптографических ключей

5.2.1 Все поступившие СКЗИ, эксплуатационная и техническая документация к ним должны быть взяты на поэкземплярный учет по журналу поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним (Приложение № 1). При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

5.2.2 Поэкземплярный учет СКЗИ имеет цель обеспечить контроль за снабжением СКЗИ, их наличием, движением, расходом, и исключить обезличенное пользование ими. В журнале поэкземплярного учета должно отражаться полное прохождение каждого в отдельности экземпляра СКЗИ, эксплуатационной и технической документации к ним с момента получения до уничтожения.

5.2.3 Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, ведет ответственный пользователь СКЗИ.

5.2.4 Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, выдаются под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

5.2.5 При увольнении, перемещении пользователя СКЗИ, все числящие за ним СКЗИ и другие документы передаются по акту (Приложение № 2) работнику, которому поручено исполнять его обязанности.

5.2.6. СКЗИ, эксплуатационная и техническая документация должны находиться в металлических шкафах, оборудованных замками, гарантирующих надежную защиту от несанкционированного доступа.

5.2.7 Криптосредства и ключевые документы могут доставляться фельдьегерской связью или со специально выделенными оператором ответственными пользователями СКЗИ и сотрудниками академии при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки. Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 7 из 16
--	---	-------------------------------------

5.2.8 Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается, и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

5.2.9 Полученные упаковки вскрывают пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю.

5.2.10 При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует вернуть изготовителю для установления причин произошедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний изготовителя.

5.2.11 Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме.

5.2.12 СКЗИ уничтожают (утилизируют) в соответствии с требованиями эксплуатационной и технической документации к ним.

5.2.13 Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятными из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

5.2.14 Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

5.2.15 СКЗИ, ключевые документы, должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета.

5.2.16 О факте уничтожения криптографических ключей составляется акт об уничтожении криптографических ключей (Приложение № 3).

5.2.17 К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 8 из 16
--	---	-------------------------------------

- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

5.2.18 В случае возникновения обстоятельств, указанных в п.5.2.17 настоящей инструкции, пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации ответственному пользователю СКЗИ.

5.2.19 Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

5.2.20 Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в настоящей инструкции.

5.3 Размещение, охрана и организация режима в помещениях, где установлены СКЗИ

5.3.1 Помещения, где установлены СКЗИ или хранятся ключевые документы к ним должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещение посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению.

5.3.2 Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

5.3.3 Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает ответственный пользователь СКЗИ по согласованию, при необходимости, с оператором, в помещениях которого установлены криптосредства или хранятся ключевые документы к ним. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны.

5.3.4 Двери помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

5.3.5 Для предотвращения просмотра извне помещений, их окна должны быть защищены.

5.3.6 Для хранения ключевых документов, эксплуатационной и технической документации, устанавливающих криптосредства носителей, должно быть предусмотрено наличие надежных металлических хранилищ, оборудованных внутренними замками.

5.3.7 По окончании рабочего дня помещение, где установлены СКЗИ и хранятся ключевые документы к ним должны быть закрыты.

5.3.8 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 9 из 16
--	---	-------------------------------------

быть немедленно сообщено ответственному пользователю СКЗИ. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

5.3.9 Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.3.10 На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи.

5.4 Контроль за организацией, обеспечением функционирования и безопасности СКЗИ

5.4.1 Контроль за организацией, обеспечением функционирования и безопасности СКЗИ ведется в целях получения объективных оценок уровня защиты информации с использованием криптографических средств и своевременного принятия необходимых мер по повышению безопасности системы.

5.4.2 Контроль за организацией, обеспечением функционирования и безопасности СКЗИ в академии осуществляется ответственным пользователем СКЗИ в пределах своих служебных полномочий.

6 Внесение изменений

Внесение изменений в настоящую инструкцию производит разработчик в соответствии с требованиями п. 7.2.9 ДП СМК 02-01-2013.

7 Рассылка

Разослать:

1-й экз. – разработчику;

2-й экз. остальные экземпляры согласно листа рассылки.

8 Приложения

Приложение 1 – Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Приложение 2 – Акт приема – передачи средств криптографической защиты информации.

Приложение 3 – Акт об уничтожении криптографических ключей и ключевых документов.



ФГБОУ ВПО Самарская ГСХА
Положение о деятельности
СМК 04-18-2014

Издание 2014-09

Лист 10 из 16

8 Приложения

Приложение 1 – Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Приложение 2 – Акт приема – передачи средств криптографической защиты информации.

Приложение 3 – Акт об уничтожении криптографических ключей и ключевых документов.

Разработчик:

директор центра
информационных технологий

В.А. Киров

Согласовано:

проректор по учебной работе

И.Н. Гужин

начальник юридического отдела

А.И. Стольников

начальник отдела качества образования

Е.С. Казакова

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 11 из 16
---	---	--------------------------------------

Приложение 1

**ЖУРНАЛ ПОЭКЗЕМПЛЯРНОГО УЧЕТА СКЗИ, ЭКСПЛУАТАЦИОННОЙ
И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ**

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийный номер СКЗИ эксплуатационной и технической документации к ним, ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов		
ФИО сотрудников органа криптографической защиты	Дата подключения (установки) и подписи лиц, производивших их подключение	Номера аппаратных средств, в которые установлены СКЗИ	Дата изъятия (уничтожения)	ФИО сотрудников органа криптографической защиты	Номер акта или расписка об уничтожении
9	10	11	12	13	14

	<p align="center">ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014</p>	<p align="center">Издание 2014-09</p>
		<p align="center">Лист 12 из 16</p>

Приложение 2

АКТ
№ _____ от «___» _____ 201_года
приема-передачи

Мы, нижеподписавшиеся, _____ и _____ в связи с убытием в _____ (отпуск и т.п.), на основании требований «Инструкцией по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационной системе персональных данных «Абитуриент», составили настоящий акт в том, что первый сдал, а второй принял нижеперечисленные СКЗИ, дела, журналы и документы:

- 1.
- 2.
- 3.

Всего подлежит передаче _____ (прописью) наименования.

Сдал: _____
(подпись)

Принял: _____
(подпись)

НЕУЧТЕННЫЙ ЭКЗЕМПЛЯР

	ФГБОУ ВПО Самарская ГСХА Положение о деятельности СМК 04-18-2014	Издание 2014-09 Лист 13 из 16
---	---	--------------------------------------

Приложение 3

АКТ № _____
об уничтожении криптографических ключей и ключевых документов.

от «___» _____ 201_г.

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечание
1	2	3	4	5	6	7	8

Всего уничтожено (_____) криптографических ключей на (_____) ключевых носителях. Записи акта сверены с записями в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

НЕУЧТЕННЫЙ ЭКЗЕМПЛЯР



ФГБОУ ВПО Самарская ГСХА
Положение о деятельности
СМК 04-18-2014

Издание 2014-09

Лист 15 из 16

ЛИСТ ОЗНАКОМЛЕНИЯ

	Подразделение академии	Дата ознакомления	Фамилия И.О. руководителя СП	Подпись
1	Отдел кадров			
2	Деканат агрономического факультета			
3	Деканат факультета биотехнологий и ветеринарной медицины			
4	Деканат инженерного факультета			
5	Деканат технологического факультета			
6	Деканат экономического факультета			
7	Институт управленческих технологий и аграрного рынка			
8	Заочный факультет			
9				
10				
11				
12				

НЕУЧТЕННЫЙ ЭКЗЕМПЛЯР

