УТВЕРЖДЕНО

Приказом Директора "МА СКПК «Единство»"

\_\_\_\_\_\_\_\_подпись\_\_\_\_\_\_\_\_/ Зимин В.И.

"11" ноября 2020 г.

ПОЛОЖЕНИЕ

о конфиденциальной информации

(коммерческой тайне) и информационной безопасности

межрегиональной Ассоциации сельскохозяйственных

кредитных потребительских кооперативов «Единство»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Гражданским [кодексом](consultantplus://offline/ref=C242E3D8C66AFBA6D763A7EC4D40C4F4756A8D23D0A4B269117EC296F3A3sAH) Российской Федерации, Федеральным [законом](consultantplus://offline/ref=C242E3D8C66AFBA6D763A7EC4D40C4F474678B21D7A3B269117EC296F3A3sAH) от 29.07.2004 N 98-ФЗ "О коммерческой тайне" и иными федеральными законами и нормативными правовыми актами Российской Федерации для урегулирования отношений, связанных с установлением, изменением и прекращением режима коммерческой тайны в межрегиональной Ассоциации сельскохозяйственных кредитных потребительских кооперативов «Единство» (далее -Организация, Работодатель).

Настоящее Положение вступает в действие с даты утверждения соответствующим приказом руководителя Организации.

1.2. Определения, употребляемые в настоящем Положении:

1.2.1. Конфиденциальная информация (информация, составляющая коммерческую тайну) - сведения любого характера (производственные, технические, экономические, организационные и другие), а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

1.2.2. Обладатель конфиденциальной информации - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

1.2.3. Разглашение конфиденциальной информации - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

1.3. В целях охраны конфиденциальности информации Работодатель обязан:

1.3.1. Ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются Работодатель и его контрагенты.

1.3.2. Ознакомить под расписку работника с установленным Работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение.

1.3.3. Создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

1.4. В целях охраны конфиденциальности информации Организации работник обязан:

1.4.1. Выполнять установленный Работодателем режим коммерческой тайны.

1.4.2. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются Работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях.

1.4.3. Передать Работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну, либо уничтожить такую информацию или удалить ее с этих материальных носителей под контролем Работодателя.

1.4.4. Об утрате или недостаче документов, содержащих закрытую информацию, ключей от сейфов (хранилища, шкафа и т.п.), печатей, пропусков и т.п. немедленно сообщать своему непосредственному руководителю или лицу, его замещающему.

1.5. Ответственным за обеспечение конфиденциальности информации в Организации является руководитель Организации.

2. ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ

КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ ОРГАНИЗАЦИИ

2.1. Конфиденциальной информацией Организации являются:

2.1.1. Сведения по вопросам управления, кадровым, штатным, правовым вопросам и вопросам региональной и межрегиональной политики Организации, если раскрытие такой информации не предусмотрено нормативными актами Банка России.

2.1.2. Сведения по экономической, финансовой и бухгалтерской деятельности Организации если раскрытие такой информации не предусмотрено нормативными актами Банка России.

.

2.1.3. Сведения по коммерческой деятельности на внутреннем рынке Организации если раскрытие такой информации не предусмотрено нормативными актами Банка России.

2.1.4. Сведения по вопросам внешнеэкономической деятельности Организации если раскрытие такой информации не предусмотрено нормативными актами Банка России.

2.2. Режим коммерческой тайны не может быть установлен в отношении сведений, перечисленных в [ст. 5](consultantplus://offline/ref=C242E3D8C66AFBA6D763A7EC4D40C4F474678B21D7A3B269117EC296F33A8983510556FE1849413AAEs8H) Федерального закона от 29.07.2004 N 98-ФЗ "О коммерческой тайне" и информации, раскрываемой Организацией в соответствии с требованиями Банка России.

.

3. ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Меры по охране конфиденциальности информации, принимаемые руководителем Организации, должны включать в себя:

1) ограничение доступа к информации, составляющей коммерческую тайну;

2) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

4. ПОРЯДОК ДОПУСКА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. По всем вопросам деятельности Организации допуск к конфиденциальной информации имеет руководитель Организации.

4.2. По вопросам, относящимся к их компетенции, к конфиденциальной информации Организации имеют допуск следующие лица:

- руководитель Организации;

- заместители руководителя Организации;

- начальник отдела отчетности и проверок Организации;

- юрисконсульт и специалист Организации;

- бухгалтер Организации;

- работники, в трудовом договоре которых имеется соответствующее условие о неразглашении конфиденциальной информации и(или) подписавшие соответствующее обязательства;

- иные лица, получившие допуск к конфиденциальной информации Организации в соответствии с настоящим Положением.

4.3. Организация по мотивированному требованию Банка России, органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую конфиденциальную информацию. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено действующим законодательством Российской Федерации.

5. ХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

И КОНТРОЛЬ ЗА ПОРЯДКОМ ДОПУСКА И РАБОТЫ С НЕЙ

5.1. Хранение конфиденциальной информации осуществляется по месту нахождения офисов Организации и(или) ее структурных подразделений, а также на электронных средствах (носителях) информации.

5.2. Контроль за порядком допуска и работы с конфиденциальной информацией осуществляет руководитель (директор) Организации.

5.3. При осуществлении контроля лицо, указанное в [п. 5.3](#Par88) настоящего Положения, проверяет:

- состояние офиса;

- наличие носителей конфиденциальной информации.

6. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Общие положения по информационной безопасности

6.1.1. Обеспечение информационной безопасности включает комплекс повседневно проводимых мероприятий, а именно:

* допуск (предоставление прав доступа) к информации, средствам информатизации и в помещения;
* доступ к информации, средствам информатизации и в помещения;
* содержание средств информатизации;
* обеспечение безопасности информации;
* использование средств защиты информации;
* контроль состояния информационной безопасности;

6.2. Допуск

Допуск – это комплекс мероприятий, проводимых с целью предоставления прав доступа сотрудникам Организации, представителям сторонних организаций и посетителям в помещения, к средствам информатизации и к информации Организации;

Право предоставления допуска имеет только руководитель Организаци.

6.2.1. Допуск может предоставляться:

* сотрудникам Организации;
* сотрудникам сторонних организаций, выполняющим работы по заказу (договору) Организации;
* сотрудникам государственных органов, Банка России, имеющим соответствующие полномочия;
* членам Организации и(или) посетителям.

6.2.3. Различаются постоянный и временный (разовый) допуск. Постоянный допуск предоставляется только сотрудникам Организации или представителям сторонних организаций, выполняющим работы по договору. Временный (разовый) допуск предоставляется как сотрудникам Организации, так и иным лицам, в том числе членам Организации и(или) посетителям.

6.2.4. Порядок действий по предоставлению допуска зависит от того, к какому объекту допускается лицо, какова категория этого объекта, постоянный это допуск или разовый и кому он предоставляется: сотруднику Организации, представителю сторонней организации или члену/посетителю.

6.2.5. Допуск оформляется в форме устного и/или письменного распоряжения Директора Организаци. Должностные лица Организации (штатные сотрудники) имеют допуск ко всей информации Организации.

6.2.6. Срок постоянного допуска – ограничен сроком работы сотрудника в Организации.

6.2.7. Постоянный допуск сотрудникам сторонних организаций, выполняющим работы по договору, предоставляется Директором Организаци при условии, что в договоре предусмотрены обязательства контрагента по выполнению требований информационной безопасности и сохранению коммерческой тайны.

6.2.8. Временный (разовый) допуск предоставляется Директором Организации устно:

* сотрудникам сторонних организаций, выполняющих работы по договору, - на основании предварительной договоренности с контрагентом;
* членам и посетителям – соответствующим письменным распоряжением (приказом) Директора Организации.

Представителям государственных органов и Банка России может быть предоставлен допуск к любым объектам информационной системы, но только временный (разовый) и в строгом соответствии с имеющимися у них полномочиями.

6.3. Доступ

Доступ – это совокупность действий, выполняемых сотрудниками Организации:

* с целью получения возможности использования информации;
* с целью предоставления возможности использования информации сотрудниками сторонних организаций, государственных органов, Банка России, членов Организации и посетителями.

Таким образом, *действия по доступу выполняются только сотрудниками* Организации, даже если допускаются иные лица.

6.3.1. Общая задача доступа подразделяется на подзадачи:

* доступ в помещения;
* доступ к средствам информатизации;
* доступ к программным продуктам и информации.

Действия по осуществлению доступа подразделяются на организационные и технические.

6.3.2. Ответственность за организацию доступа несет Директор Организации, а за правильное выполнение действий по доступу – сотрудник, их выполняющий.

*6.4. Доступ в помещения*

Доступ в помещения сотрудников, чьи рабочие места находятся в этих помещениях, осуществляется в соответствии с Правилами внутреннего трудового распорядка в Организации.

Доступ в помещения сотрудников Организации в рабочие дни и часы – свободный.

По устному распоряжению Директора Организации доступ также может осуществляться в нерабочие часы и дни.

Доступ в помещения Организации сотрудников сторонних организаций и представителей государственных органов, Банка России возможен только при наличии соответствующего допуска через того из сотрудников Организации, к которому этот посетитель прибыл.

6.4.1. Доступ в помещения Организации контролируется с использованием систем контроля и доступа собственником помещений, занимаемых Организацией. Нахождение в помещениях Организации кого бы то ни было, кроме сотрудников, без сопровождения сотрудников (в рабочее время) или сотрудников собственника помещений (в нерабочее время, в том числе в случае возникновения непредвиденных ситуаций) строго запрещается.

Технические действия по доступу в помещения зависят от того, оборудованы ли помещения соответствующими техническими средствами и, как правило, состоят в снятии помещения с контроля системой охранной сигнализации и вскрытие помещения установленным порядком в начале рабочего дня.

6.4.2. Организационные действия по доступу в помещения выполняются сотрудниками Организации, и заключаются в:

* проверке состояния помещения и находящихся в нем средств информатизации при вскрытии помещения и перед его закрытием;
* принятии мер по недопущению в помещения посторонних лиц, не имеющих допуска или нарушающих правила доступа;

6.4.3. Порядок доступа в помещения сотрудников арендодателя:

в случаях прямой необходимости, в рабочее время - вместе с сотрудником, работающим в данном помещении, в нерабочее время - с последующим составлением служебной записки на имя директора Организации (если доступ в помещение был осуществлен в присутствии сотрудника Организаци) с изложением причин доступа и описанием состояния помещения;

*6.5. Доступ к средствам информатизации*

Доступ к средствам информатизации, находящимся на рабочих местах сотрудников (далее – «ответственные за средства информатизации»), осуществляется этими сотрудниками без ограничений.

Доступ к средствам информатизации, представителей сторонних организаций, представителей государственных органов, банка России, членов Организации и(или) посетителей осуществляется только при наличии допуска. При этом непосредственное использование средства информатизации осуществляется сотрудником, ответственным за него, а лицо, получившее доступ, присутствует при этом;

*6.5.1. Средства информатизации* Организации могут быть подключены *к ресурсам и сервисам международной компьютерной сети Internet*. Локальная вычислительная сеть, имеющая в своём составе средства информатизации также может иметь выход в международную сеть Internet.

6.5.2. Технические действия по осуществлению доступа заключаются в:

* включении питания;
* преодолении установленным порядком имеющихся средств защиты доступа (замок, вход по паролю, идентификация пользователя и др.).

6.5.3. После того, как операции по доступу к средствам выполнены, ответственный за средство информатизации обязан обеспечить невозможность использования средства кем-либо, кроме него самого. Запрещается даже на короткое время оставлять без контроля средство информатизации, если такая возможность не исключена технически.

6.5.4. Для доступа к средствам информатизации там, где это возможно, в обязательном порядке должен использоваться пароль.

*6.6. Доступ к программным продуктам и информации*

Порядок получения доступа к программным продуктам и информации определяется порядком доступа в помещения и к средствам информатизации. Ответственность за правильность доступа к программным продуктам и информации несут сотрудники Организации, на рабочих местах которых используются эти программные средства и информация.

6.6.1. Доступ к программным продуктам и информации обеспечивается:

* к программным продуктам и компьютерной информации – имеющимися программно-аппаратными средствами защиты;
* к информации на бумажных носителях – принятой технологией несекретного «бумажного» делопроизводства;
* к речевой, видео- и другим видам информации – мерами обеспечения доступа в помещения и к средствам связи.
* Технические действия по доступу к программным продуктам и информации заключаются в:
* запуске программного продукта;
* преодолении установленным порядком имеющихся программных и аппаратных средств защиты;
* регистрации доступа средствами регистрации, если они имеются.

6.6.2. Содержание средств информатизации

Правильное с точки зрения информационной безопасности содержание (эксплуатация и хранение) средств информатизации предполагает предотвращение несанкционированного их использования.

Содержание программных продуктов средств информатизации определяется содержанием технических средств информатизации (компьютеров, сетей), на которых эти программные продукты установлены.

6.6.3. Средства информатизации содержатся, как правило, на рабочих местах сотрудников, за которыми эти средства закреплены.

6.6.4. В рабочее время ответственность за содержание средств информатизации несут сотрудники, за которыми эти средства закреплены, а в их отсутствие – лица, исполняющие их обязанности и/или функции. В нерабочее время ответственность за хранение средств информатизации несет собственник помещений, занимаемых Организации в соответствии с соответствующим договором и/или охранное предприятие.

6.6.5. Приемка в эксплуатацию средств информатизации (аппаратных, программных) проводится силами сотрудников Организации и/или подрядчиком (сотрудниками подрядчиков), с которым Организацией заключены соответствующие договоры (контракты), следующим образом:

* средство информатизации оснащается программными продуктами, устанавливается на рабочем месте и проверяется;
* производится проверка безопасности средства информатизации; при необходимости для такой проверки могут привлекаться специализированные организации;
* средство информатизации, при необходимости, дополняется средствами защиты информации, из него исключаются не используемые «опасные» устройства;
* средство проверяется сотрудниками Организации на предмет готовности к эксплуатации;
* Сотрудник, ответственный за содержание средства информатизации, в части обеспечения информационной безопасности обязан:
* обеспечить установленный порядок доступа к средству информатизации;
* правильно использовать средства защиты информации, с которыми работает средство информатизации, если они имеются;
* при обнаружении признаков несанкционированного доступа к средству информатизации немедленно прекратить все работы с ним, обеспечить сохранение его в текущем состоянии и сообщить о случившемся Директору Организации.
* Учет средств информатизации ведется бхгалтером Организации:
* технические средства информатизации учитываются в соответствии с их инвентарными номерами, которые присваиваются им при приобретении (установке, вводе в эксплуатацию);
* программные продукты средств информатизации учитываются поэкземплярно.

6.6.6. Дистрибутивы программных продуктов хранятся таким образом, чтобы исключить возможность использования их для инсталляции несанкционированных копий программного продукта. Инсталляцию прикладных и автономных программных продуктов выполняет сотрудник Организации и/или подрядчик (сотрудник подрядчика), с которым Организацией заключены соответствующие договоры (контракты).

6.6.7. Рабочие копии программных продуктов должны быть защищены от несанкционированной модификации программного кода и данных, для чего должны применяться различные методы, в том числе:

* установка программных продуктов на средствах информатизации;
* установка программных продуктов на серверах сети с разделением доступа к ним;
* защита программных продуктов от копирования;
* шифрование исполняемых модулей и данных программных продуктов на носителях информации;

6.6.8. Если доступ к средству информатизации защищается устройствами типа «замок» (механические замки, электронные замки, кодовые устройства и т.п.), имеющими «ключи» (обычные ключи, магнитные карты и т.п.), то оригинал ключа хранится у ответственного сотрудника, а дубликаты – у руководителя Организации. Хранение оригинала и дубликатов должно быть обеспечено таким образом, чтобы исключить возможность попадания ключа к кому-либо, кроме этих лиц.

6.9. Обеспечение безопасности информации

Безопасность информации обеспечивается и предполагает:

* полное исключение возможности несанкционированного доступа к ней;
* исключение возможности несанкционированной модификации, предупреждение возможности анализа и статистической оценки.

6.9.1. Основой безопасности информации является доступ в помещения, к средствам информатизации и самой информации. Кроме этого, в зависимости от формы представления информации, с целью обеспечения ее безопасности принимаются специальные меры, изложенные ниже. Во всех случаях, за исключением специально оговоренных, ответственность за принятие этих мер несет сотрудник, использующий информацию или организующий мероприятие с ее использованием.

6.9.2. Безопасность информации в бумажной форме представления обеспечивается в соответствии с принятой технологией «бумажного» документооборота.

6.9.3. Для обеспечения безопасности речевой информации необходимо:

* ограничить число лиц, участвующих в переговорах, до минимально необходимого;
* проводить переговоры в местах, исключающих возможность подслушивания;
* применять специальные средства, если такие имеются.
* Для обеспечения безопасности телефонных переговоров необходимо:
* безусловно ограничить обсуждение при ведении переговоров по открытым (незащищенным) телефонным линиям связи сведения, относящиеся к коммерческой тайне и служебной информации;
* применять специальные средства, если такие имеются.
* Для обеспечения безопасности информации, обрабатываемой с помощью средств информатизации необходимо:
* обеспечить защиту от несанкционированного получения информации, содержащей коммерческую тайну и/или служебную информацию, и защиту от модификации, а также возможность восстановления авторства доступа к такой информации, для чего в обязательном порядке применять все меры защиты, доступные на используемых программно-аппаратных средствах;
* обеспечить хранение носителей информации (дискет, магнито-оптических дисков, компакт-дисков и др.) с информацией, содержащей коммерческую тайну и/или служебную информацию, способом, исключающим их утрату, несанкционированное копирование и получение;
* обеспечить хранение применяемых средств защиты информации, в том числе средств доступа к ним, способом, исключающим их несанкционированное использование.

6.10. Использование средств защиты информации

Средства защиты информации – это специальные технические средства, используемые для предупреждения несанкционированного использования всех видов информации. Разнообразие видов используемой информации, целей защиты, вариантов угроз, применяемых технологий защиты определяют широкую номенклатуру таких средств. В каждом случае необходимости защиты информации выбирается свой конкретный тип средства.

6.10.1. По вариантам использования различаются средства защиты информации:

* коллективные, применяемые для защиты информации, используемой одновременно несколькими (многими) сотрудниками;
* индивидуальные, применяемые только одним сотрудником для защиты информации, используемой им самим;
* сетевые, применяемые для защиты в вычислительных сетях и сетях связи.

6.10.2. Необходимость применения средств защиты информации определяется Директором Организации, при принятии решения о применении информационной техники и в других случаях. Принятие решения на применение средств защиты (в том числе сетевых средств защиты), выбор способа защиты и типа средства защиты информации осуществляется совместно Директором Организации и сотрудником, который использует защищаемую информацию.

6.10.3. Ответственность за использование средств защиты информации несут:

* за средства защиты коллективного пользования и сетевые средства защиты – Директор Организации;
* за средства защиты индивидуального пользования – сотрудники, на рабочих местах которых эти средства установлены;

6.10.4. Порядок приемки в эксплуатацию средств защиты информации:

* средство устанавливается сотрудником Организации и/или подрядчиком (сотрудником подрядчика) на рабочем месте и проверяется в соответствии с инструкцией по эксплуатации;
* сотрудник Организации и представитель подрядчика (в случае необходимости) производит(ят) приемку средства с проверкой функционирования, принимает меры по его эффективному использованию;
* средство защиты информации передается в эксплуатацию назначенному ответственному сотруднику.

6.10.5. Сотрудник, ответственный за средство защиты информации, обязан:

* изучить средство в объеме, необходимом для правильной его эксплуатации;
* обеспечить установленный порядок использования средства: своевременно включать и выключать его, поддерживать эффективный режим работы;
* не допускать несанкционированного применения средства кем бы то ни было, обеспечить его сохранность, сообщать Директору Организации обо всех попытках несанкционированного использования средства или подозрениях на такие попытки;
* проводить техническое обслуживание, обеспечивать его исправность, инициировать проведение ремонта в случае выхода из строя и выполнять другие эксплуатационные операции.

6.11. Контроль состояния информационной безопасности

Контроль состояния информационной безопасности проводится с целью проверки ее организации, а также предупреждения и своевременного выявления случаев ее нарушения.

6.11.1. Обязанности по контролю распределяются следующим образом:

* сотрудники контролируют текущее состояние информационной безопасности на своих рабочих местах;
* Директор Организации повседневно контролирует текущее состояние информационной безопасности в локальной вычислительной сети;

6.11.2. Директор Организации контролирует состояние информационной безопасности на отдельных участках:

* контролирует выполнение сотрудниками установленного порядка действий по доступу к объектам информационной системы;
* анализирует состояние информационной системы с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации;
* контролирует правильность использования имеющихся коллективных и индивидуальных средств информационной защиты.

6.11.3. В случае выявления каких-либо отклонений или нарушений в системе информационной безопасности Директор Организации немедленно принимает меры к их устранению самостоятельно, через подрядчика и/или исполнителя на основании соответствующего договора (контракта, соглашения).

6.11.4. Сотрудники Организации анализируют состояние своих рабочих мест с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации. В случае выявления таких попыток сотрудник немедленно обязан сообщить об этом Директору Организации.

6.12. Порядок действий в случае выявления нарушений информационной безопасности

Действия, предпринимаемые в случае выявления нарушений информационной безопасности, состоят в следующем:

* выявление факта нарушения;
* прекращение всех операций, связанных с рабочим местом (участком), на котором произошло нарушение;
* принятие экстренных мер для прекращения несанкционированного доступа или использования информации;
* оповещение о нарушении;
* восстановление работоспособности информационной системы;
* расследование причин нарушения информационной безопасности;
* проверка состояния информационной безопасности по факту нарушения.

6.12.1. Немедленно после выявления нарушения сотрудник, который обнаружил его, обязан прекратить все операции по использованию по назначению информации и средств информатизации, которые выполнялись на участке, где произошло нарушение, а также, если необходимо, на смежных участках. Если выявлен несанкционированный доступ в помещения, всякий доступ в него должен быть прекращен.

6.12.2. Если на момент выявления нарушения несанкционированный доступ или использование средств информатизации и информации еще продолжаются, сотрудник, выявивший их, обязан немедленно принять меры к их прекращению. Конкретное содержание этих мер зависит от того, каков характер нарушения, какой ущерб может быть нанесен нарушением, какие побочные последствия повлечет принятие этих мер. По возможности следует привлечь для выработки и принятия мер арендодателя, охранное предприятий, осуществляющее охрану арендуемых помещений. Ответственность за адекватность принимаемых мер несут в порядке привлечения сотрудник, выявивший нарушение, Директор Организации.

6.12.3. С целью минимизации ущерба от прекращения работы информационной системы немедленно после того, как возможность дальнейшего нарушения информационной безопасности устранена, принимаются меры для восстановления ее работы. Решение на восстановление работы принимает Директор Организации.

6.12.4. Расследование причин нарушения производится Директором Организации, при этом все связанные с нарушением сотрудники должны оказывать содействие расследованию. Целью расследования является выявление истинных причин нарушения и предпосылок к нему для принятия мер к недопущению его повторения. Расследование проводится сразу после восстановления работоспособности информационной системы, в обязательном порядке, независимо от последствий, которые повлекло нарушение. Результаты расследования могут оформляются приказом Директора Организации.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ

7.1. Лица, разгласившие конфиденциальную информацию, а также лица, нарушившие настоящее Положение, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются Работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Приложение 1 к Положению

ОБЯЗАТЕЛЬСТВО РАБОТНИКА

О СОБЛЮДЕНИИ РЕЖИМА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_МА СКПК «Единство»:

(должность)

1) ознакомлен(-а) с перечнем конфиденциальных сведений - межрегиональной Ассоциации сельскохозяйственных кредитных потребительских кооперативов «Единство» и положением о конфиденциальной информации и информационной безопасности межрегиональной Ассоциации сельскохозяйственных кредитных потребительских кооперативов «Единство»;

2) обязуюсь выполнять установленный в межрегиональной Ассоциации сельскохозяйственных кредитных потребительских кооперативов «Единство» режим конфиденциальности информации и информационной безопасности согласно положению о конфиденциальной информации и информационной безопасности межрегиональной Ассоциации сельскохозяйственных кредитных потребительских кооперативов «Единство»;

3) обязуюсь передать работодателю при прекращении или расторжении трудового договора имеющиеся в моем пользовании материальные носители информации, содержащие конфиденциальную информацию.

Подтверждаю, что я предупрежден(-а), что в соответствии со [статьей 14](consultantplus://offline/ref=6019810EDCD6EF5F9A78680624582A7A853B245E404F27A2287B44EC45A2EA72093B3C5B0BA0D812h1BAI) Федерального закона "О коммерческой тайне" в случае умышленного или неосторожного разглашения конфиденциальной информации, ставшей мне известной в связи с исполнением трудовых обязанностей, могу быть привлечен(-на) к дисциплинарной, гражданско-правовой, административной или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

"\_\_\_"\_\_\_\_\_\_\_\_ \_\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(подпись)

С данным Положением ознакомлены:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность работника) (подпись) (Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность работника) (подпись) (Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность работника) (подпись) (Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность работника) (подпись) (Ф.И.О.)