

# Общество с ограниченной ответственностью «Приволжское-Плюс»

Юридический адрес: 413102, Саратовская область, Энгельсский район, р.п.Приволжский, М/К д.27  
Телефоны: Приемная т/(факс): 75-04-94 Е-mail: ooo.privolzhskoe2012@yandex.ru

Р/с 40702810800000025114 в АО АКБ «Экспресс-Волга» г. Саратов, К/с 30101810600000000808  
БИК 046311808, ИНН/КПП 6449967595 / 644901001, ОКВЭД 70321, ОКПО 13760712

## ПРИКАЗ

От 01 октября 2014 г.

№ 03/1

*о вопросах защиты персональных  
данных в ООО «Приволжское-Плюс»*

Во исполнение Федеральных законов от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», распоряжения Губернатора Саратовской области от 28 декабря 2007 года № 109-р «О реализации Федерального закона «О персональных данных» и на основании Устава ООО «Приволжское-Плюс»:

1. Создать информационную систему персональных данных в ООО «Приволжское-Плюс» в составе согласно Приложению 1.

2. Утвердить Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Приволжское-Плюс» согласно Приложению 2.

3. Создать комиссию по классификации информационных систем персональных данных в ООО «Приволжское-Плюс» в составе согласно Приложению 3.

4. Возложить обязанности:

- организации мероприятий по защите персональных данных, обрабатываемых в информационных системах персональных данных ООО «Приволжское-Плюс» на заместителя директора Г.В. Петкилеву (ответственный за защиту информации персональных данных);

- по организации и осуществлению защиты информационных систем персональных данных, обрабатываемых на автоматизированных рабочих местах и их эксплуатацию в ООО «Приволжское-Плюс» на инженера снабжения Филину Л.А. (администратор безопасности информации).

4. Для обработки персональных данных информационных систем на автоматизированных рабочих местах директор ООО «Приволжское-Плюс» назначает

должностных лиц (пользователей) распоряжением с возложением обязанностей по обеспечению безопасности обрабатываемых персональных данных.

5. Инженеру снабжения Филиной Л.А. (администратор безопасности информации) в срок до 10 октября 2014 года:

- разработать Инструкцию администратору безопасности информации и Инструкцию пользователю по обработке персональных данных;
- организовать выполнение мероприятий по защите информации на автоматизированных рабочих местах, где обрабатываются персональные данные на информационных системах ООО «Приволжское-Плюс», обеспечив сохранность защищаемой информации;
- провести инвентаризацию информационных систем персональных данных, имеющихся в ООО «Приволжское-Плюс» и до 10 октября 2014 года составить и утвердить сводный Перечень информационных систем;
- организовать учет носителей информации (ПЭВМ), на которых хранятся персональные данные ООО «Приволжское-Плюс» и до 10 октября 2014 года разработать Инструкции о порядке обращения с данными носителями;
- определить угрозы безопасности информационных систем персональных данных администрации Приволжского муниципального образования и в срок до 10 октября 2014 года разработать Перечень актуальных угроз безопасности персональных данных и определить меры по их предотвращению.

6. Председателю комиссии по квалификации информационных систем персональных данных заместителю директора ООО «Приволжское-Плюс» Г.В. Петкилевой в срок до 10 октября 2014 года провести квалификацию каждой информационной системы персональных данных и по ее данным составить **Акты квалификации** и представить их на утверждение.

7. Контроль за исполнением настоящего постановления возложить на заместителя директора ООО «Приволжское-Плюс» Г.В. Петкилеву.

Директор  
ООО «Приволжское-Плюс»



Г.А. Слободяников



Приложение 1  
к Приказу ООО «Приволжское-Плюс»  
от «01» октября 2014 г. № 03/1

**СОСТАВ**  
**информационной системы персональных данных в ООО «Приволжское-Плюс»**

| № п/п | Наименование объекта (подразделения), адрес, фамилия и инициалы руководителя | Наименование ИСПД, способ обработки, хранения и передачи информации                                                                                     | Правовое обоснование обработки персональных данных                                                                                                                                          | Фамилия и инициалы пользовател ей |
|-------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| 1     | 2                                                                            | 3                                                                                                                                                       | 4                                                                                                                                                                                           | 5                                 |
| 1.    | Отдел кадров (инспектор отдела кадров Истрашкина Е.В.)                       | Система учета работников ПЭВМ – один.<br>Жесткий диск, бумага.                                                                                          | Трудовой кодекс РФ, Положение об отделе организационно-правовой и кадровой работы.                                                                                                          | Е.В. Истрашкина                   |
| 2.    | Отдел учета и отчетности (главный бухгалтер И.А. Васильченко.)               | Система учета и отчетности по заработной плате, персонифицированному учету ПЭВМ – один.<br>Жесткий диск, бумага.                                        | Трудовой кодекс РФ, Налоговый кодекс РФ, Приказ от 26.12.1994г. № 170 Министерства Финансов РФ «Положение о бухгалтерском учете и отчетности в РФ», Положение об отделе учета и отчетности. | И.А. Васильченко                  |
| 3.    | Отдел секретариата                                                           | Система учета выполнение работ по текущему капитальному ремонту, сметы, отчеты, жалобы, заявления, ведение сайтов ПЭВМ – один.<br>Жесткий диск, бумага. | Жилищный кодекс РФ, Постановление Правительства № 354 от 06.05.2011 г., Постановление Правительства РФ № 731 от 23.09.2010 г.                                                               | Л.И. Чугунова                     |

**ПОЛОЖЕНИЕ**  
**об обеспечении безопасности персональных данных**  
**при их обработке в информационных системах персональных данных**  
**в ООО «Приволжское-Плюс»**

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Приволжское-Плюс», представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее – информационные системы).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах ООО «Приволжское-Плюс» обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Технические и программные средства защиты должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах ООО «Приволжское-Плюс» осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических



сигналов, физических полей, носителей на бумажной, магнитной, магнитооптической и иной основе.

3. Методы и способы защиты информации в информационных системах ООО «Приволжское-Плюс» установлены в соответствии с требованиями Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах ООО «Приволжское-Плюс» оценивается при проведении государственного контроля и надзора.

4. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем ООО «Приволжское-Плюс».

5. Средства защиты информации, применяемые в информационных системах ООО «Приволжское-Плюс» должны в установленном порядке проходить процедуру оценки соответствия.

6. Информационные системы ООО «Приволжское-Плюс» классифицируются в структурных подразделениях, осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам работников ООО «Приволжское-Плюс», общества и государства в целом.

Порядок проведения классификации информационных систем ООО «Приволжское-Плюс» должен соответствовать требованиям совместного Приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

7. Обмен персональными данными при их обработке в информационных системах ООО «Приволжское-Плюс» осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

8. Размещение информационных систем ООО «Приволжское-Плюс», специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. Возможные каналы утечки информации при обработке персональных данных в информационных системах ООО «Приволжское-Плюс» определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

10. Безопасность персональных данных при их обработке в информационной системе ООО «Приволжское-Плюс» обеспечивает лицо, которому на основании распоряжения директора поручает обработку



персональных данных (далее – уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и их безопасность при обработке в информационной системе ООО «Приволжское-Плюс».

11. При обработке персональных данных в информационной системе в ООО «Приволжское-Плюс» должно быть обеспечено:

- а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передача их лицам, не имеющим права доступа к такой информации;
- б) своевременное обнаружение факторов несанкционированного доступа к такой информации;
- в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- д) постоянный контроль обеспечения уровня защищенности персональных данных.

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах в ООО «Приволжское-Плюс» включают в себя:

- а) определение угроз безопасности персональных данных при их обработке и формирование на их основе частной модели угроз;
- б) разработку на основе частной модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для третьего класса информационных систем;
- в) проверку готовности средств защиты информации к использованию с составлением заключения о возможности их эксплуатации;
- г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационно-технической документацией;
- д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
- з) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использование средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- к) описание системы защиты персональных данных.



13. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе ООО «Приволжское-Плюс» распоряжением директора назначается ответственный за обеспечение безопасности персональных данных (Администратор безопасности информации).

14. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного директором ООО «Приволжское-Плюс».

15. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 14 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в **электронном журнале обращений**. Содержание электронного журнала обращений периодически проверяется директором ООО «Приволжское-Плюс».

16. При обнаружении нарушений порядка предоставления персональных данных директор ООО «Приволжское-Плюс» или уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

17. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

18. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах ООО «Приволжское-Плюс» оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

19. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах ООО «Приволжское-Плюс» прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

20. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах ООО «Приволжское-Плюс», подлежат учету с использованием индексов или условных наименований и регистрационных номеров, которые определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Приложение 3

к Приказу ООО «Приволжское-Плюс»  
от «01» октября 2014 г. № 03/1

**СОСТАВ**

**комиссии по классификации информационных систем персональных данных  
ООО «Приволжское-Плюс»**

**Председатель комиссии:**

Петкилева Г.В – заместитель директора

**Секретарь комиссии:**

Филина Л.А. – администратор  
безопасности информации

**Члены комиссии:**

Васильченко И.А. - главный бухгалтер  
отдела учета и отчетности

Истрашкина Е.В. - инспектор отдела  
кадров



*Общество с ограниченной ответственностью*  
**«Приволжское-Плюс»**

Юридический адрес: 413102, Саратовская область, Энгельсский район, р.п.Приволжский, М/К д.27  
Телефоны: Приемная т/(факс): 75-04-94 E-mail: ooo.privolzhskoe2012@yandex.ru

Р/с 40702810800000025114 в АО АКБ «Экспресс-Волга» г. Саратов, К/с 30101810600000000808  
БИК 046311808, ИНН/КПП 6449967595 / 644901001, ОКВЭД 70321, ОКПО 13760712

**ПРИКАЗ**

**01 октября 2014 г.**

**№ 03/2**

*о назначении ответственного за  
обеспечение безопасности  
персональных данных*

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе ООО «Приволжское-Плюс» назначает ответственным за обеспечение безопасности персональных данных (администратор безопасности информации) инженера снабжения - Филину Любовь Александровну.

Директор  
ООО «Приволжское-Плюс»



Г.А.Слободяников

С приказом ознакомлен и согласен:

« 01 » 10 2014 г. Филина Л.А. ( Филина Л.А. )

# Общество с ограниченной ответственностью «Приволжское-Плюс»

Юридический адрес: 413102, Саратовская область, Энгельский район, р.п.Приволжский, М/К д.27

Телефоны: Приемная т/(факс): 75-04-94 E-mail: ooo.privolzhskoe2012@yandex.ru

Р/с 40702810800000025114 в АО АКБ «Экспресс-Волга» г. Саратов, К/с 30101810600000000808  
БИК 046311808, ИНН/КПП 6449967595 / 644901001, ОКВЭД 70321, ОКПО 13760712

## ПРИКАЗ

01 октября 2014 г.

№ 03/3

*о назначении ответственного за  
защиту информации  
персональных данных*

Для организации мероприятий по защите персональных данных, обрабатываемых в информационной системе персональных данных ООО «Приволжское» назначить ответственным за защиту информации персональных данных заместителя директора ООО «Приволжское-Плюс» - Петкилеву Галину Владимировну.

Директор  
ООО «Приволжское-Плюс»



Г.А.Слободяников

С приказом ознакомлен и согласен:

« 01 » 10 2014 г.

*(Handwritten signature)* (Петкилева Г.В.)



Общество с ограниченной ответственностью

# «Приволжское-Плюс»

Юридический адрес: 413102, Саратовская область, Энгельский район, р.п.Приволжский, М/К д.27

Телефоны: Приемная т/(факс): 75-04-94 E-mail: ooo.privolzhskoe2012@yandex.ru

Р/с 40702810800000025114 в АО АКБ «Экспресс-Волга» г. Саратов, К/с 30101810600000000808  
БИК 046311808, ИНН/КПП 6449967595 / 644901001, ОКВЭД 70321, ОКПО 13760712

## ПРИКАЗ

08 октября 2014 г.

№ 05/1

об утверждении списка  
лиц, осуществляющих  
обработку персональных данных

Утвердить список лиц, доступ которых к персональным данным, обрабатываемым в информационной системе ООО «Приволжское-Плюс», необходим для выполнения служебных обязанностей, согласно Приложению.

Директор  
ООО «Приволжское-Плюс»



Г.А. Слободяников

С приказом ознакомлены и согласны:

|      |    |         |                |                              |
|------|----|---------|----------------|------------------------------|
| «08» | 10 | 2014 г. | <i>Метов</i>   | ( <i>Метрашкина Е.В.</i> )   |
| «08» | 10 | 2014 г. | <i>Скв</i>     | ( <i>Сквирова С.Н.</i> )     |
| «08» | 10 | 2014 г. | <i>М. Сел.</i> | ( <i>Касимовичева М.А.</i> ) |
| «08» | 10 | 2014 г. | <i>Чу</i>      | ( <i>Чурикова Н.В.</i> )     |
| «08» | 10 | 2014 г. | <i>Сел</i>     | ( <i>Селюкова Т.В.</i> )     |

СПИСОК  
лиц, осуществляющих обработку персональных данных в информационной системе  
ООО «Приволжское-плюс»

| № п/п | Отдел                    | Ф.И.О. пользователя, должность            |
|-------|--------------------------|-------------------------------------------|
| 1.    | Отдел кадров             | Истрашкина Е.В. — инспектор отдела кадров |
| 2.    | Отдел учета и отчетности | Васильченко И.А. - главный бухгалтер      |
| 3.    | Отдел секретариата       | Чугунова Л.И. - секретарь                 |





УТВЕРЖДАЮ  
Директор  
ООО «Приволжское-Плюс»

Г.А. Слободяников

«08» октября 2014 г.

### СПИСКИ

сотрудников, допущенных к обработке персональных данных на автоматизированных рабочих местах в ООО «Приволжское-Плюс»

#### 1. Автоматизированное рабочее место № 1 (отдел кадров)

| № п/п | Ф.И.О.                        | Должность               |
|-------|-------------------------------|-------------------------|
| 1.    | Истрашкина Елена Владимировна | Инспектор отдела кадров |

#### 2. Автоматизированное рабочее место № 2 (отдел учета и отчетности) - система учета и отчетности по заработной плате, персонифицированного учета

| № п/п | Ф.И.О.                          | Должность         |
|-------|---------------------------------|-------------------|
| 1.    | Васильченко Ирина Александровна | Главный бухгалтер |

#### 3. Автоматизированное рабочее место № 3 (секретариат)

| № п/п | Ф.И.О.                    | Должность |
|-------|---------------------------|-----------|
| 1.    | Чугунова Людмила Ивановна | Секретарь |

Ответственный за обеспечение безопасности  
персональных данных при их обработке в  
информационных системах персональных данных

Г.В. Петкилева



УТВЕРЖДАЮ

Директор ООО «Приволжское-Плюс»

«Приволжское-Плюс»

Г.А.Слободяников

«08» октября 2014 г.

## **ИНСТРУКЦИЯ** **пользователю по обработке персональных данных** **на автоматизированных рабочих местах в ООО «Приволжское-Плюс»**

### **1. Общие положения**

Настоящая инструкция разработана в соответствии с требованиями распоряжения директора ООО «Приволжское-Плюс» от 01 октября 2014 года № 03/1 «Вопросы защиты персональных данных в ООО «Приволжское-Плюс».

Пользователями автоматизированных рабочих мест являются сотрудники, допущенные решением директора ООО «Приволжское-Плюс» к обработке персональных данных на автоматизированных рабочих местах.

### **2. Функции**

Основными функциями пользователя являются:

2.1. Выполнение мероприятий, направленных на предотвращение неправомерного доступа лиц к защищаемой информации.

2.2. Обеспечение установленного режима обработки персональных данных на автоматизированных рабочих местах.

2.3. Комиссионное удаление защищаемой информации с машинных носителей совместно с руководителем структурного подразделения администрации и ответственным за осуществление защиты информационных систем персональных данных, обрабатываемых на автоматизированных рабочих местах, и их эксплуатацию в ООО «Приволжское-Плюс» (администратором безопасности).

2.4. Вывод (запись) данных, полученных на основе защищаемой информации, либо данных, содержащих защищаемую информацию, на печать или съемные машинные носители информации (МНИ).

2.5. Проверка новых данных на отсутствие вирусов.

2.6. Ведение учета работы пользователя автоматизированной системы в соответствующем журнале учета.

2.7. Ведение учета съемных носителей информации с персональными данными в соответствующих журналах учета.

### **3. Функциональные обязанности**

3.1. Каждый сотрудник, участвующий в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированных рабочих мест (далее АРМ), несет персональную ответственность за свои действия и обязан:

3.1.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АРМ.

3.1.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ.



3.1.3. В случае неисправности средств защиты информации от несанкционированного доступа, выявление попыток несанкционированного доступа к защищаемой информации, либо обнаружения следов вскрытия технических средств, входящих в состав автоматизированного рабочего места, немедленно прекратить работу, ограничить доступ в помещение, поставить в известность администратора безопасности информации и ответственного за организацию, координацию и контроль проведения мероприятий по защите персональных данных, обрабатываемых в информационных системах персональных данных в ООО «Приволжское-Плюс».

3.1.4. Регулярно производить смену личного пароля доступа (не реже 1 раза в 6 месяцев).

3.1.5. Передавать для хранения установленным порядком свои реквизиты разграничения доступа только руководителю своего подразделения. **Запрещается сообщать кому-либо свой пароль доступа!**

3.1.6. Выполнять требования по антивирусной защите в части, касающейся действий пользователей. Проверять все новые данные, вводимые со съемных МНИ, на отсутствие вирусов.

3.1.7. Немедленно вызывать администратора безопасности (ответственного за защиту информационных систем) информации и ставить в известность начальника своего подразделения в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к ресурсам АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.) АРМ, а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных техническим паспортом АРМ отводов кабелей и подключенных устройств.

### **3.2. Пользователям категорически ЗАПРЕЩАЕТСЯ:**

3.2.1. Использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях.

3.2.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные техническим паспортом АРМ.

3.2.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

3.2.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках, компакт-дисках, флэш-накопителях, внешних ЖМД и т.п.).

3.2.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты информации от НСД. Передавать включенную ПЭВМ другому исполнителю без перезагрузки.

3.2.6. Оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.

3.2.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность администратора безопасности информации и руководителя своего подразделения, эксплуатирующего АРМ.

#### 4. Порядок действий пользователя при работе.

##### 4.1. Общие положения и требования:

4.1.1. Обработка персональных данных разрешается на основании распоряжения директора.

4.1.2. На период обработки защищаемой информации в помещении, в котором расположены автоматизированные рабочие места, могут находиться только лица, допущенные к обрабатываемой информации.

4.1.3. В начале и по окончании работы проверить сохранность печатей системного блока ПЭВМ.

4.1.4. Ввод информации со съемных МНИ осуществляется только после их проверки антивирусными средствами, которые должны периодически обновляться.

4.1.5. Файлы с защищаемой информацией должны храниться только в установленных для этого каталогах (разделах). Запрещается перенос (копирование) файлов в каталоги (разделы) с открытой информацией.

4.1.6. По окончании обработки защищаемой информации или при передаче управления другому допущенному пользователю необходимо уничтожить остаточную и ненужную информацию на жестком магнитном диске ПЭВМ или съемных МНИ.

При утере пароля или электронного идентификатора **НЕМЕДЛЕННО** прекратить работу, поставить в известность администратора безопасности информации и ответственного за организацию, координацию и контроль, проведение мероприятий по защите персональных данных, обрабатываемых в информационных системах персональных данных в ООО «Приволжское-Плюс».

С инструкцией ознакомлены:

|                             |                                   |
|-----------------------------|-----------------------------------|
| <u>08.10.2014</u><br>(дата) | <u>инициаторок</u><br>(должность) |
| <u>08.10.2014</u><br>(дата) | <u>М. Бугаев</u><br>(должность)   |
| <u>08.10.2014</u><br>(дата) | <u>секретарь</u><br>(должность)   |

|                          |                                              |
|--------------------------|----------------------------------------------|
| <u>Май</u><br>(подпись)  | <u>Морозкина Е.В.</u><br>(инициалы, фамилия) |
| <u>М.В.</u><br>(подпись) | <u>Басманов М.В.</u><br>(инициалы, фамилия)  |
| <u>Чуп</u><br>(подпись)  | <u>Чупово А.И.</u><br>(инициалы, фамилия)    |





УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»  
Г.А.Слободяников  
«08» октября 2014 г.

## ИНСТРУКЦИЯ

**по внесению изменений в списки пользователей и наделению их полномочиями доступа к информационным ресурсам автоматизированного рабочего места по обработке персональных данных по ООО «Приволжское-Плюс»**

### 1. Общие положения.

1.1. Настоящая Инструкция устанавливает порядок внесения изменений в списки пользователей и порядок наделения их полномочиями по доступу к информационным ресурсам аттестованных автоматизированных рабочих мест в ООО «Приволжское-Плюс». Пользователями автоматизированных рабочих мест являются сотрудники, допущенные к обработке персональных данных соответствующим решением директора ООО «Приволжское-Плюс».

1.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на автоматизированных рабочих местах, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя) под которым он будет регистрироваться, и работать на автоматизированном рабочем месте.

1.3. Использование несколькими сотрудниками при работе в автоматизированных рабочих местах одного и того же имени пользователя («группового имени») **ЗАПРЕЩЕНО**.

1.4. Каждому пользователю автоматизированных рабочих мест предоставляются права по доступу к информационным ресурсам и соответствующие полномочия. Права определяют, к каким конкретно информационным ресурсам (программы, файлы, массивы, архивы, базы данных и т.п.) допускается конкретный сотрудник. Полномочия определяют, что конкретно (читать, удалять, создавать) может делать допущенный к информационным ресурсам сотрудник.

### 2. Порядок внесения изменений в список пользователей.

2.1. В соответствии с должностными обязанностями сотрудников директор ООО «Приволжское-Плюс» определяет сотрудников, которых необходимо допустить к информационным ресурсам автоматизированных рабочих мест.

2.2. Необходимость допуска сотрудника к информационным ресурсам автоматизированных рабочих мест отражается в заявке руководителя структурного подразделения на имя директора ООО «Приволжское-Плюс».

2.3. На основании **заявки** производится регистрация (**создание учетной записи**) пользователя и предоставление (или изменение) ему прав доступа к ресурсам автоматизированных рабочих мест.

2.4. В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам АРМ ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на АРМ).

2.5. Заявка утверждается главой администрации.

2.6. Утвержденная заявка является основанием администратору безопасности информации для регистрации пользователя в системе защиты информации от несанкционированного доступа (СЗИ НСД) и допуска его к информационным ресурсам автоматизированного рабочего места. Заявки подшиваются и хранятся вместе с аттестационной документацией АРМ.

2.7. В случае изменения статуса сотрудника учетная запись пользователя в СЗИ НСД немедленно блокируется администратором безопасности информации. Решение о дальнейшем использовании защищаемых ресурсов, принадлежащих пользователю и хранящихся в определенных для него каталогах, принимается комиссией, в состав которой должны входить представители подразделения, эксплуатирующего автоматизированное рабочее место и администратор безопасности информации. По результатам работы комиссии составляется акт, который является основанием администратору безопасности информации для уничтожения информационных ресурсов пользователя либо для передачи этих ресурсов другому пользователю.

Администратор безопасности информации



Л.А. Филина





УТВЕРЖДАЮ

Директор ООО «Приволжское-Плюс»

Г.А.Слободяников

«08» октября 2014 г.

## ИНСТРУКЦИЯ

**по порядку установки нового общесистемного, прикладного и специального программного обеспечения на автоматизированных рабочих местах по обработке персональных данных в ООО «Приволжское-Плюс»**

### 1. Порядок внесения изменений в программное обеспечение

1.1. Изменения в состав программных средств автоматизированных рабочих мест могут вноситься только с лицензионных дистрибутивных дисков, имеющих сертификат качества. Устанавливаемое программное средство должно иметь необходимую эксплуатационную документацию.

1.2. Основанием для внесения изменений в программную среду является служебная записка от **пользователя** на имя директора ООО «Приволжское-Плюс» с указанием наименования программного средства и обоснованием необходимости его использования при выполнении задания пользователя. Ответственность за обоснование необходимости внесения изменений в программную среду и использование нового программного средства несет пользователь.

1.3. Перед установкой нового программного средства пользователь совместно с администратором безопасности информации производит антивирусный контроль дистрибутива.

1.4. Отладочные и экспериментальные работы (апробирование программ) производится с применением не конфиденциальной (условной) информации на автоматизированном рабочем месте. После установки программного средства осуществляется проверка его функционирования и составляется **акт ввода в эксплуатацию**, который подписывается членами комиссии и утверждается директором ООО «Приволжское-Плюс».

Акт ввода в эксплуатацию нового программного средства хранится совместно с документацией автоматизированного рабочего места.

1.5. В случае обнаружения не декларированных (не описанных документации) возможностей программного средства, пользователь немедленно сообщает администратору безопасности информации. Дальнейшее использование программного средства до получения специальных указаний прекращается.

1.6. Пользователь в части его касающейся, обязан знать документацию на программное средство и уметь правильно его эксплуатировать. Ознакомление и обучение пользователя работе с программным средством в пределах выполняемых функций проводит администратор безопасности информации.

1.7. Начальная установка и настройка программного средства осуществляется администратором безопасности информации согласно эксплуатационной документации.

1.8. Настройка прав доступа к устанавливаемому программному средству при использовании в составе автоматизированного рабочего места системы защиты информации от несанкционированного доступа (СЗИ НДС) выполняется администратором безопасности информации в соответствии с разрешительной системы доступа пользователя к информационным ресурсам автоматизированного рабочего места.

## **2. Порядок проверки работоспособности СЗИ НДС после установки новых программных средств на автоматизированном рабочем месте.**

2.1. При установке нового программного средства администратор безопасности информации обязан:

- установить права доступа пользователя к файлам программного средства в соответствии с разрешительной системой доступа пользователя к информационным ресурсам автоматизированного рабочего места;
- средствами СЗИ НДС подсчитать контрольные суммы файлов программных средств (при необходимости);
- если для пользователя, использующего установленное программное средство, установлен режим замкнутой программной среды, необходимо средствами СЗИ НДС добавить в список разрешенных ему для запуска программ исполняемые модули данного пакета.

2.2. После осуществления данных действий необходимо проверить корректность функционирования СЗИ НДС, для чего требуется произвести следующие действия:

- для каждого пользователя автоматизированного рабочего места, для которого установлен режим замкнутой программной среды, требуется проверить работоспособность установленного программного средства и сохранение режима замкнутой программной среды;
- в режиме обычного пользователя необходимо проверить возможность изменения вновь установленных (обновленных) файлов;
- для каждого пользователя необходимо проверить (при необходимости) разграничение доступа к вновь установленным (обновленным) файлам.

2.3. После установки нового программного средства администратор безопасности информации обязан проверить работоспособность автоматизированного рабочего места и правильность настройки СЗИ НДС, установленной на ПЭВМ.

Администратор безопасности информации \_\_\_\_\_ Л.А. Филина





УТВЕРЖДАЮ

Директор ООО «Приволжское-Плюс»

Г.А.Слободяников

«08» октября 2014 г.

## ИНСТРУКЦИЯ

**по организации парольной защиты на автоматизированных рабочих  
местах обработки персональных данных в ООО «Приволжское-Плюс»**

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) на автоматизированных рабочих местах (далее АРМ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности информации на ООО «Приволжское-Плюс».

1.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самовольно с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов для всех классов безопасности. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем по 4 позициям;

- личный пароль пользователь не имеет права сообщать никому.

1.4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

1.5. Полная плановая смена паролей пользователей должна производиться регулярно, **не реже одного раза в 6 месяцев**. Периодичность смены пароля обеспечивается соответствующей настройкой средств защиты информации несанкционированного доступа (далее – СЗИ НСД).

1.6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться администратором безопасности информации немедленно после окончания последнего сеанса работы данного пользователя с системой.

1.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри администрации и другие обстоятельства) администратора безопасности информации, которому по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АРМ.

1.8. В случае компрометации личного пароля пользователям автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.1.4 или 1.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

1.9. Хранение пользователем значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

1.10. Повседневный контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации, периодический контроль возлагается на ответственного за организацию, координацию и контроль проведения мероприятий по защите персональных данных, обрабатываемых в информационных системах персональных данных в ООО «Приволжское-Плюс»

Администратор безопасности информации



Л.А. Филина





УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»

Г.А.Слободяников  
«08» октября 2014 г.

## ИНСТРУКЦИЯ

**администратору безопасности (ответственному по осуществлению защиты информационных систем персональных данных) автоматизированных рабочих мест в ООО «Приволжское-Плюс»**

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности организует выполнение мероприятий по защите информации на автоматизированных рабочих местах, обрабатывающих персональные данные в ООО «Приволжское-Плюс», обеспечивает сохранность защищаемой информации, настройку системы защиты информации от несанкционированного доступа (СЗИ НСД) в соответствии с разрешительной системой доступа пользователей к информационным ресурсам автоматизированных рабочих мест.

1.2. Администратор безопасности назначается и освобождается от исполнения обязанностей приказом директора ООО «Приволжское-Плюс».

1.3. В практической деятельности администратор безопасности информации руководствуется требованиями приказа директора ООО «Приволжское-Плюс» «О вопросах защиты персональных данных в ООО «Приволжское-Плюс» от 01 октября 2014 года № 03/1 и настоящей должностной Инструкцией.

### 2. ОСНОВНЫЕ ФУНКЦИИ

Основными функциями администратора безопасности являются:

2.1 Организация работ по предотвращению неправомерного доступа лиц к защищаемой информации.

2.2 Выявление возможных каналов утечки защищаемой информации за счет несанкционированного доступа к информации в процессе деятельности и внесение предложений по их закрытию.

2.3. Установка, настройка и поддержание в исправном состоянии технических и программных средств автоматизированных рабочих мест в ООО «Приволжское-Плюс».

Настройка и эксплуатация технических и программных средств защиты информации от несанкционированного доступа.

2.4. Регистрация пользователей в системе, присвоение или изменение полномочий доступа пользователей к ресурсам автоматизированных рабочих мест в соответствии с разрешительной системой доступа к информационным ресурсам.

2.5. Контроль соответствия действий пользователей с заданиями на работы.

2.6. Резервное копирование системной информации автоматизированных рабочих мест, ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

2.7. Обновление программного обеспечения автоматизированных рабочих мест, проверка целостности данных.

2.8. Проверка системы автоматизированных рабочих мест на отсутствие вирусов.

### 3. ПРАВА И ОБЯЗАННОСТИ

### Администратор безопасности обязан:

3.1 Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.2 Знать перечень автоматизированных рабочих мест, предназначенных для обработки персональных данных, и перечень задач, решаемых с их использованием в ООО «Приволжское-Плюс».

3.3 Совместно с ответственными по организации, координации и контролю проведения мероприятий по защите персональных данных организовывать разработку и обеспечение выполнения мер по защите информации при ее обработке на автоматизированных рабочих местах.

3.4 Осуществлять настройку системы защиты информации от несанкционированного доступа в соответствии с установленным классом защищенности и разрешительной системой доступа пользователей к информационным ресурсам автоматизированных рабочих мест.

3.5 В случаях неисправности или нарушения целостности средств защиты информации от несанкционированного доступа (далее – СЗИ НСД), выявления попыток несанкционированного доступа к защищаемой информации, либо обнаружения следов вскрытия основных технических средств и систем (далее – ОТСС) автоматизированных рабочих мест – немедленно прекратить работу, ограничить доступ в помещение и поставить в известность ответственного по организации, координации и контролю проведения мероприятий по защите персональных данных.

3.6 В случае выявления неквалифицированных действий пользователей, не несущих в себе угроз для безопасности информации, поставить в известность об этом ответственного по организации, координации и контролю проведения мероприятий по защите персональных данных, временно заблокировать возможность работы этого пользователя и организовать дополнительные занятия с ним.

3.7 Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию автоматизированных рабочих мест.

3.8 Контролировать соответствие состава автоматизированных рабочих мест реальным конфигурациям и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения на автоматизированных рабочих местах).

3.9 Хранить, осуществлять прием и выдачу персональных идентификаторов пользователей (при их наличии), осуществлять контроль правильности использования персональных идентификаторов пользователями автоматизированных рабочих мест.

3.10 Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования автоматизированных рабочих мест и осуществления НСД к информации и техническим средствам автоматизированных рабочих мест. При выявлении таковых сообщать о них ответственному по организации, координации и контролю проведения мероприятий по защите персональных данных.

3.11 Проводить инструктаж пользователей автоматизированных рабочих мест по правилам работы с используемой СЗИ НСД.

3.12 При увольнении пользователей оперативно изменять учетные реквизиты защиты: пароли, идентификаторы (если это необходимо).

3.13 При изменении программной среды или пользователей проводить тестирование всех функций СЗИ НСД, имитируя попытки НСД.

3.14 В случае необходимости обновлять эксплуатируемое либо устанавливать новое программное обеспечение.

3.15 Проверять в соответствии с Инструкцией все новые данные на отсутствие вирусов. Регулярно обновлять базы данных антивирусных средств.



3.16 Не реже одного раза в год проводить тестирование всех функций СЗИ НСД с помощью специальных программных средств.

#### **Администратор безопасности информации имеет право:**

4.1 Требовать от пользователей автоматизированных рабочих мест соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации.

4.2 Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов автоматизированных рабочих мест.

4.3 Обращаться к ответственному по организации, координации и контролю проведения мероприятий по защите персональных данных с требованием прекращения работы пользователя на автоматизированном рабочем месте при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности информации.

4.4 Выступать с предложениями по совершенствованию мер защиты информации.

4.5 Обращаться к ответственному по организации, координации и контролю проведения мероприятий по защите персональных данных для оказания необходимой технической и методологической помощи в своей работе.

#### **Ответственность администратора безопасности**

5.1 На администратора безопасности информации возлагается **персональная ответственность за качество проводимых им работ по обеспечению защиты информации**, обрабатываемой на автоматизированных рабочих местах.

5.2 Администратор безопасности информации **отвечает за соответствие настройки СЗИ НСД требованиям установленных для автоматизированных рабочих мест классов защищенности.**

5.3 Администратор безопасности информации **несет ответственность** по действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

#### **Порядок администрирования работы на автоматизированных рабочих местах**

6.1 Работа с СЗИ НСД должна осуществляться в соответствии с комплектом документации СЗИ НСД.

6.2 Проанализировать работу пользователей на автоматизированных рабочих местах. Обращать особое внимание на попытки осуществления "скрытого" несанкционированного переноса (копирования) защищаемой информации на любые носители (разделы, каталоги). Характерными признаками осуществления таких действий является работа с защищаемой информацией и создание (редактирование) файлов на других носителях (разделах, каталогах в пределах одного сеанса работы).

6.3 Проанализировать полномочия каждого пользователя автоматизированных рабочих мест, соответствие их значений ранее установленным.

6.4 Проанализировать и убедиться в неизменности программной среды автоматизированных рабочих мест. На ПЭВМ автоматизированных рабочих мест должны отсутствовать средства разработки и отладки программ.

Администратор безопасности информации



Л.А. Филина



УТВЕРЖДАЮ

Директор ООО «Приволжское-Плюс»

Плюс»

Г.А.Слободяников

«08» октября 2014 г.

## ИНСТРУКЦИЯ

### по проведению антивирусного контроля на автоматизированных рабочих местах по обработке персональных данных по ООО «Приволжское-Плюс»

1.1. Настоящая инструкция определяет требования к организации защиты автоматизированных рабочих мест от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников ООО «Приволжское-Плюс», эксплуатирующих автоматизированные рабочие места, за выполнение этих требований.

1.2. К использованию на автоматизированных рабочих местах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и согласованных с администратором безопасности информации ООО «Приволжское-Плюс». Установка средств антивирусного контроля на автоматизированных рабочих местах осуществляется администратором безопасности информации. Настройка параметров средств антивирусного контроля осуществляется администратором безопасности информации в соответствии с руководствами инструкции по применению конкретных антивирусных средств.

### 1.3. Применение средств антивирусного контроля.

1.3.1. Перед началом работы на ПЭВМ пользователь обязан проверить свои рабочие папки на жестком магнитном диске (ЖМД), собственные рабочие съемные машинные носители информации (МНИ) на отсутствие вирусов с помощью штатных средств антивирусной защиты.

1.3.2. Обязательному антивирусному контролю подлежит любая получаемая и передаваемая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях (дискетах, компакт-дисках, флэш-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на системный носитель).

1.3.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться **не реже одного раза в месяц**.

1.3.4. Вновь устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка жестких дисков ПЭВМ.



#### 1.4. Действия пользователя при подозрении наличия компьютерного вируса.

1.4.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание фактов, частное появление сообщений о системных ошибках и т.п.) пользователи автоматизированных рабочих мест самостоятельно или вместе с ответственным за осуществление защиты информационных систем персональных данных и их эксплуатации ООО «Приволжское-Плюс» (администратором безопасности информации) должны провести внеочередной антивирусный контроль ПЭВМ.

1.4.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за безопасность информации (администратора безопасности информации).

1.4.3. Ответственный за безопасность информации (администратор безопасности информации) обязан:

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- по факту обнаружения зараженных вирусом файлов пользователь обязан составить служебную записку на имя директора ООО «Приволжское-Плюс», в которой необходимо указать предположительный источник (отправителя, владельца и т.д.). Зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

#### 1.5. Ответственность

1.5.1. Ответственность за организацию антивирусного контроля на автоматизированных рабочих местах в соответствии с требованиями настоящей Инструкции возлагается на ответственного за организацию координации и контроль проведения мероприятий по защите персональных данных.

1.5.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на администратора безопасности информации и пользователя автоматизированного рабочего места.

1.5.3. Периодический контроль за состоянием антивирусной защиты в автоматизированных рабочих местах, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции пользователем осуществляется администратором безопасности информации.

Администратор безопасности информации                     Л.А. Филина



УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»

Г.А. Слободяников  
«08» октября 2014 г.

**АКТ № 1**  
**классификации информационной системы персональных данных**  
**в ООО «Приволжское-Плюс»**

от «08» октября 2014 г.

В соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02. 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», комиссия в составе:

- Председателя комиссии: - Г.В. Петкилевой – заместителя директора  
Секретаря комиссии: - Л.А. Филиной - администратора безопасности информации  
Членов комиссии: - И.А. Васильченко – главного бухгалтера  
- Е.В. Истрашкиной - инспектора отдела кадров

**УСТАНОВИЛА:**

1. Информационная система находится в кабинете № 5 – отдел кадров ООО «Приволжское-Плюс» (Саратовская обл., Энгельсский р-н, р.п. Приволжский, ул. Мясокомбинат, д. 27).

Информационная система персональных данных состоит из автоматизированного рабочего места на основе одного ПЭВМ (тип настольный), используемой только для хранения информации и базы данных на магнитных и бумажных носителях.

Рабочее место является автономным, режим обработки персональных данных – однопользовательский.



Передача персональных данных на магнитных носителях третьим лицам и организациям не осуществляется.

Для защиты персональных данных предусмотрены следующие мероприятия:

- вход в базу данных компьютера защищен **паролем** пользователя;
- бумажные носители персональных данных хранятся в сейфе, закрываемом на замок;
- выдача (передача) бумажных носителей, содержащих персональные данные, осуществляется по журналу (книге) учета;
- помещение, в котором обрабатываются персональные данные, по окончании рабочего дня закрывается на замок, помещение сдается под охрану.

2. В информационной системе обрабатываются следующие персональные данные сотрудников организации, не имеющих статуса юридического лица: персональные данные, позволяющие идентифицировать субъекта персональных данных (Ф.И.О., место жительства, паспортные данные, имущественное и социальное положение, состояние о здоровье, образование, сведения о заработной плате и др.) Указанные персональные данные (**Хпд**) могут быть отнесены к 3 категории персональных данных.

3. По объему в информационной системе обрабатываются персональные данные субъектов персональных данных в пределах организации (в виде карточек, бланков, сведений, справок и т.п.) - (**Хипд**), что соответствует **3 категории персональных данных**.

Исходя из вышеизложенного, настоящую информационную систему персональных данных можно отнести к классу **К - 3**.

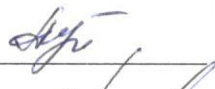
Нарушение заданной характеристики безопасности персональных данных данной информационной системы может привести к незначительным негативным последствиям для субъектов персональных данных.

Председатель комиссии:



Г.В. Петкилева

Секретарь комиссии:

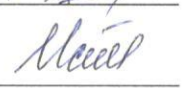


Л.А. Филина

Члены комиссии:



И.А. Васильченко



Е.В. Истрашкина



УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»

Г.А. Слободяников  
«08» октября 2014 г.

**АКТ № 2**  
**классификации информационной системы персональных данных**  
**в ООО «Приволжское-Плюс»**

от «08» октября 2014 г.

В соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02. 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», комиссия в составе:

- |                        |                                                         |
|------------------------|---------------------------------------------------------|
| Председателя комиссии: | - Г.В. Петкилевой – заместителя директора               |
| Секретаря комиссии:    | - Л.А. Филиной - администратора безопасности информации |
| Членов комиссии:       | - И.А. Васильченко – главного бухгалтера                |
|                        | - Е.В. Истрашкиной - инспектора отдела кадров           |

**УСТАНОВИЛА:**

1. Информационная система находится в кабинете № 5 – отдел учета и отчетности ООО «Приволжское-Плюс» (Саратовская обл., Энгельсский р-н, р.п. Приволжский, ул. Мясокомбинат, д. 27).

Информационная система персональных данных состоит из автоматизированного рабочего места на основе одного ПЭВМ (тип: настольный, используемой только для хранения информации и базы данных на магнитных и бумажных носителях.

Рабочее место является автономным, режим обработки персональных данных – однопользовательский.



Передача персональных данных на магнитных носителях третьим лицам и организациям не осуществляется.

Для защиты персональных данных предусмотрены следующие мероприятия:

- вход в базу данных компьютера защищен **паролем** пользователя;
- бумажные носители персональных данных хранятся в сейфе, закрываемом на замок;
- выдача (передача) бумажных носителей, содержащих персональные данные, осуществляется по журналу (книге) учета;
- помещение, в котором обрабатываются персональные данные, по окончании рабочего дня закрывается на замок, помещение сдается под охрану.

2. В информационной системе обрабатываются следующие персональные данные сотрудников организации, не имеющих статуса юридического лица: персональные данные, позволяющие идентифицировать субъекта персональных данных (Ф.И.О., место жительства, паспортные данные, имущественное и социальное положение, образование, сведения о заработной плате и др.) Указанные персональные данные (**Хпд**) могут быть отнесены к 3 категории персональных данных.

3. По объему в информационной системе обрабатываются персональные данные субъектов персональных данных в пределах организации (в виде карточек, бланков, сведений, справок и т.п.) - (**Хппд**), что соответствует **3 категории персональных данных**.

Исходя из вышеизложенного, настоящую информационную систему персональных данных можно отнести к классу **К - 3**.

Нарушение заданной характеристики безопасности персональных данных данной информационной системы может привести к незначительным негативным последствиям для субъектов персональных данных.

Председатель комиссии:



Г.В. Петкилева

Секретарь комиссии:



Л.А. Филина

Члены комиссии:



И.А. Васильченко



Е.В. Истрашкина



УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»

Г.А. Слободяников  
«08» октября 2014 г.

**АКТ № 3**  
**классификации информационной системы персональных данных**  
**в ООО «Приволжское-Плюс»**

от «08» октября 2014 г.

В соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02. 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», комиссия в составе:

- Председателя комиссии: - Г.В. Петкилевой – заместителя директора  
Секретаря комиссии: - Л.А. Филиной - администратора безопасности информации  
Членов комиссии: - И.А. Васильченко – главного бухгалтера  
- Е.В. Истрашкиной - инспектора отдела кадров

**УСТАНОВИЛА:**

1. Информационная система находится в кабинете № 2 – секретариат ООО «Приволжское-Плюс» (Саратовская обл., Энгельсский р-н, р.п. Приволжский, ул. Мясокомбинат, д. 27).

Информационная система персональных данных состоит из автоматизированного рабочего места на основе одного ПЭВМ (тип: настольный, используемой только для хранения информации и базы данных на магнитных и бумажных носителях.

Рабочее место является автономным, режим обработки персональных данных – однопользовательский.



Передача персональных данных на магнитных носителях третьим лицам и организациям не осуществляется.

Для защиты персональных данных предусмотрены следующие мероприятия:

- вход в базу данных компьютера защищен **паролем** пользователя;
- бумажные носители персональных данных хранятся в сейфе, закрываемом на замок;
- выдача (передача) бумажных носителей, содержащих персональные данные, осуществляется по журналу (книге) учета;
- помещение, в котором обрабатываются персональные данные, по окончании рабочего дня закрывается на замок, помещение сдается под охрану.

2. В информационной системе обрабатываются следующие персональные данные: персональные данные, позволяющие идентифицировать субъекта персональных данных (Ф.И.О., место жительства, номер лицевого счета и др.) Указанные персональные данные (**Хпд**) могут быть отнесены к 3 категории персональных данных.

3. По объему в информационной системе обрабатываются данные менее 1000 субъектов персональных данных - (**Хппд**), что соответствует 3 категории персональных данных.

Исходя из вышеизложенного, настоящую информационную систему персональных данных можно отнести к классу **К - 3**.

Нарушение заданной характеристики безопасности персональных данных данной информационной системы может привести к незначительным негативным последствиям для субъектов персональных данных.

Председатель комиссии:



Г.В. Петкилева

Секретарь комиссии:



Л.А. Филина

Члены комиссии:



И.А. Васильченко



Е.В. Истрашкина



УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»  
Г.А.Слободяников  
«08» октября 2014 г.

**ПЕРЕЧЕНЬ**  
**защищаемых информационных ресурсов персональных данных**  
**автоматизированного рабочего места № 1**  
**на базе ПЭВМ**

отдела организационно-правовой и кадровой работы  
ООО «Приволжское-Плюс»

1. Выходные документы программы 1С – зарплата и управление персоналом (ЗУП) на бумажных носителях.
2. Выходные документы реестра работников на бумажных носителях.
3. Файлы со сведениями реестра сотрудников на жестком диске, бумаге.

Ответственный за организацию, координацию  
и контроль проведения мероприятий по защите  
персональных данных

Г.В.Петкилева





УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»  
Г.А.Слободяников  
«08» октября 2014 г.

**ПЕРЕЧЕНЬ**  
**защищаемых информационных ресурсов персональных данных**  
**автоматизированного рабочего места № 2**  
на базе ПЭВМ  
отдела учета и отчетности ООО «Приволжское-Плюс»

1. Выходные документы программы 1С – зарплата и управление персоналом (ЗУП) на бумажных носителях.
2. Файлы с расчетами заработной платы на жестком диске, бумаге.

Ответственный за организацию, координацию  
и контроль проведения мероприятий по защите  
персональных данных

 Г.В. Петкилева



УТВЕРЖДАЮ

Директор ООО «Приволжское-Плюс»

Г.А.Слободяников

«08» октября 2014 г.

**ПЕРЕЧЕНЬ**  
**защищаемых информационных ресурсов персональных данных**  
**автоматизированного рабочего места № 3**  
**на базе ПЭВМ**  
**секретариат ООО «Приволжское-Плюс»**

1. Входящие и исходящие документы, сметы, заявления граждан, отчеты на бумажных носителях, ведение сайта организации.
2. Файлы на жестком диске и на бумаге.

Ответственный за организацию, координацию  
и контроль проведения мероприятий по защите  
персональных данных

Г.В. Петкилева





УТВЕРЖДАЮ  
Директор ООО «Приволжское-Плюс»  
Г.А.Слободяников  
«08» октября 2014 г

**ПЕРЕЧЕНЬ**  
**носителей, на которых хранятся персональные данные в ООО «Приволжское-Плюс»**

1. **Отдел кадров**

| №<br>п/п | Вид носителя, фирма производитель, серийный номер,<br>инвентарный номер                      | Описание ИСПДн<br>(наименование, класс)      | Ф.И.О.<br>сотрудников-<br>пользователей |
|----------|----------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| 1.       | Жесткий диск ПЭВМ                                                                            | Система учета<br>работников<br><br>Класс: КЗ | Истрашкина<br>Е.В.                      |
| 2.       | Флэш-накопитель<br><br>Фирма производитель:<br><br>Серийный номер:<br><br>Инвентарный номер: |                                              |                                         |
| 3.       | Дискета<br><br>Фирма производитель:<br><br>Серийный номер:<br><br>Инвентарный номер:         |                                              |                                         |
| 4.       | База данных на бумажных носителях                                                            |                                              |                                         |

2. **Отдел учета и отчетности**

| №<br>п/п | Вид носителя, фирма производитель, серийный номер,<br>инвентарный номер | Описание ИСПДн<br>(наименование, класс)                                                                 | Ф.И.О.<br>сотрудников-<br>пользователей |
|----------|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------|
| 1.       | Жесткий диск ПЭВМ                                                       | Система учета и<br>отчетности по<br>заработной плате,<br>персонифицированного<br>учета<br><br>Класс: КЗ | Васильченко<br>И.А                      |
| 2.       | Флэш-накопитель<br><br>Фирма производитель:                             |                                                                                                         |                                         |

|    |                                                                          |             |  |
|----|--------------------------------------------------------------------------|-------------|--|
|    | Серийный номер:<br>Инвентарный номер:                                    |             |  |
| 3. | Дискета<br>Фирма производитель:<br>Серийный номер:<br>Инвентарный номер: | отсутствует |  |
| 4. | База данных на бумажных носителях                                        |             |  |

### 3. Отдел секретариата

| №<br>п/п | Вид носителя, фирма производитель, серийный номер,<br>инвентарный номер          | Описание ИСПДн<br>(наименование, класс)                         | Ф.И.О.<br>сотрудников-<br>пользователей |
|----------|----------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------|
| 1.       | Жесткий диск ПЭВМ                                                                | Система учета и отчетности по обслуживанию МКД<br><br>Класс: КЗ | Чугунова Л.И.                           |
| 2.       | Флэш-накопитель<br>Фирма производитель:<br>Серийный номер:<br>Инвентарный номер: |                                                                 |                                         |
| 3.       | Дискета<br>Фирма производитель:<br>Серийный номер:<br>Инвентарный номер:         |                                                                 |                                         |
| 4.       | База данных на бумажных носителях                                                |                                                                 |                                         |

Администратор безопасности информации  Л.А. Филина



Общество с ограниченной ответственностью

# «Приволжское-Плюс»

Юридический адрес: 413102, Саратовская область, Энгельсский район, р.п.Приволжский, М/К д.27  
Телефоны: Приемная тл/(факс): 75-04-94 E-mail: ooo.privolzhskoe2012@yandex.ru

Р/с 40702810800000025114 в АО АКБ «Экспресс-Волга» г. Саратов, К/с 30101810600000000808  
БИК 046311808, ИНН/КПП 6449967595 / 644901001, ОКВЭД 70321, ОКПО 13760712

## ПРИКАЗ

12 августа 2015 г.

№ 32/1

об утверждении списка  
лиц, осуществляющих  
обработку персональных данных

Внести изменения в список лиц, доступ которых к персональным данным, обрабатываемым в информационной системе ООО «Приволжское-Плюс», необходим для выполнения служебных обязанностей.

И утвердить измененный список лиц, доступ которых к персональным данным, обрабатываемым в информационной системе ООО «Приволжское-Плюс», необходим для выполнения служебных обязанностей, согласно Приложению.

Директор  
ООО «Приволжское-Плюс»



Г.А. Слободяников

С приказом ознакомлены и согласны:

|         |         |              |                             |
|---------|---------|--------------|-----------------------------|
| «12» 08 | 2015 г. | <i>Мейер</i> | ( <i>Метракидзе Е.В.</i> )  |
| «12» 08 | 2015 г. | <i>Сид</i>   | ( <i>Гущина С.А.</i> )      |
| «12» 08 | 2015 г. | <i>В. Л.</i> | ( <i>Васильченко М.А.</i> ) |
| «12» 08 | 2015 г. | <i>Сид</i>   | ( <i>Сидорова Т.В.</i> )    |
| «12» 08 | 2015 г. | <i>Семех</i> | ( <i>Семехово И.А.</i> )    |

Приложение

СПИСОК  
лиц, осуществляющих обработку персональных данных в информационной системе  
ООО «Приволжское-плюс»

| № п/п | Отдел                    | Ф.И.О. пользователя, должность            |
|-------|--------------------------|-------------------------------------------|
| 1.    | Отдел кадров             | Истрашкина Е.В. — инспектор отдела кадров |
| 2.    | Отдел учета и отчетности | Васильченко И.А. - главный бухгалтер      |
| 3.    | Отдел секретариата       | Смехнова Н.А. - секретарь                 |





УТВЕРЖДАЮ  
Директор  
ООО «Приволжское-Плюс»

Г.А. Слободяников

«12» августа 2015 г.

### СПИСКИ

сотрудников, допущенных к обработке персональных данных на автоматизированных рабочих местах в ООО «Приволжское-Плюс»

#### 1. Автоматизированное рабочее место № 1 (отдел кадров)

| № п/п | Ф.И.О.                        | Должность               |
|-------|-------------------------------|-------------------------|
| 1.    | Истрашкина Елена Владимировна | Инспектор отдела кадров |

#### 2. Автоматизированное рабочее место № 2 (отдел учета и отчетности) - система учета и отчетности по заработной плате, персонифицированного учета

| № п/п | Ф.И.О.                          | Должность         |
|-------|---------------------------------|-------------------|
| 1.    | Васильченко Ирина Александровна | Главный бухгалтер |

#### 3. Автоматизированное рабочее место № 3 (секретариат)

| № п/п | Ф.И.О.                         | Должность |
|-------|--------------------------------|-----------|
| 1.    | Смехнова Наталия Александровна | Секретарь |

Ответственный за обеспечение безопасности  
персональных данных при их обработке в  
информационных системах персональных данных

Г.В. Петкилева