ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
МОСКОВСКОЙ ОБЛАСТИ
ЛОТОШИНСКИЙ ЦЕНТР ЗАНЯТОСТИ НАСЕЛЕНИЯ

УТВЕРЖДАЮ
Директор Государственного
казенного учреждения
Московской области
Лотошинского центра
занятости населения
С.Н. Федотов

«25» 03 2016 г.

П О Л О Ж Е Н И Е
О ЗАЩИТЕ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения:

Настоящее положение разработано в соответствии с требованиями законодательных и нормативных правовых актов Российской Федерации по защите информации и обеспечению безопасности персональных данных и Методическими рекомендациями Комитета по труду и занятости населения Московской области.

Организация защиты информации и обеспечение безопасности персональных данных в Государственном казенном учреждении Московской области Лотошинском центре занятости населения (далее – центр занятости) представляет собой принятие организационных и технических мер, направленных на обеспечение защиты информации от несанкционированного доступа к ней с целью копирования, распространения, уничтожения, модифицирования, блокирования, а также от иных неправомерных действий в отношении защищаемой информации.

Ответственность за организацию защиты информации и обеспечение безопасности персональных данных в центре занятости возлагается на директора центра занятости.

Общее руководство системой защиты информации в центре занятости и ее совершенствованием, контроль за выполнением требований, установленных законодательными и нормативными правовыми актами по защите информации и обеспечению безопасности персональных данных, возлагаются на одного из заместителей директора центра занятости или подготовленного специалиста из числа штатных работников центра занятости (далее - администратор безопасности информации).

Ответственность за организацию выполнения установленных правил эксплуатации защищаемых объектов информатизации и соблюдения требований по защите информации работниками структурных подразделений центра занятости возлагается на руководителей соответствующих структурных подразделений, в ведении которых находятся объекты информатизации и информационные ресурсы, подлежащие защите.

Ответственность за соблюдение требований по безопасности защищаемой информации и эксплуатации основных и вспомогательных технических средств на автоматизированных рабочих местах, исключение возможностей компрометации средств идентификации пользователей и криптографической защиты информации возлагается на работников центра занятости, допущенных к обработке защищаемой информации и защищенным объектам информатизации (далее – пользователь).

Непосредственное техническое сопровождение (подключение, установка, настройка) средств вычислительной техники (далее – СВТ) и средств защиты информации возлагается на подготовленного специалиста из числа штатных работников центра занятости (далее – системный администратор).

Для оказания услуг в области защиты информации центром занятости могут привлекаться специализированные организации, имеющие лицензию на данный вид деятельности, без допуска их специалистов к защищаемой информации.

Требования настоящего Положения доводятся в части, касающейся работникам центра занятости под роспись.

2. Защищаемая информация:

2.1. В центре занятости подлежат защите:

персональные данные работников центра занятости;

персональные данные субъектов, обратившихся в центр занятости за получением государственных услуг в сфере труда и занятости населения;

персональные данные, содержащиеся в обращениях граждан;

информация ограниченного доступа с пометкой «Для служебного пользования».

2.2. Обработка информации, подлежащей защите, осуществляется на автоматизированных рабочих местах и без использования средств автоматизации.

3. Организационные и технические меры защиты информации:

3.1. Обеспечение защиты персональных данных от несанкционированного доступа к ним с целью копирования, распространения, уничтожения, изменения и иных неправомерных действий осуществляется в общей системе защиты информации центра занятости с учетом требований законодательных и нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Порядок разработки, оформления, учета и хранения документов, магнитных и машинных носителей информации с пометкой «Для служебного пользования», а также их уничтожения определяется Инструкцией о порядке обращения с документами, содержащими информацию ограниченного доступа, с пометкой «Для служебного пользования», утверждаемой директором центра занятости.

3.3. Основные мероприятия по организации защиты информации и обеспечению безопасности персональных данных:

издание приказа об организации защиты информации и обеспечении безопасности персональных данных;

определение перечня автоматизированных рабочих мест и автоматизированных информационных систем, предназначенных для обработки защищаемой информации;

разработка Положения о разрешительной системе доступа к защищаемой информации;

утверждение списка работников, допускаемых к обработке защищаемой информации, с указанием перечня информационных ресурсов и прав доступа;

определение контролируемой зоны, в пределах которой исключается бесконтрольное нахождение лиц, не допущенных к обработке защищаемой информации и средствам информатизации, предназначенным для обработки такой информации;

определение актуальных угроз безопасности информации;

проведение классификации автоматизированных рабочих мест и автоматизированных информационных систем, предназначенных для обработки защищаемой информации, с целью установления методов и способов обеспечения ее защиты в соответствии с актуальными угрозами безопасности информации;

установка сертифицированных по требованиям безопасности программных и аппаратно-программных средств защиты информации, обеспечивающих ее техническую защиту в соответствии с результатами классификации;

разработка Технического паспорта на каждую защищаемую информационную систему или отдельное (не входящее в систему) автоматизированное рабочее место, предназначенное для обработки защищаемой информации;

определение и утверждение обязанностей (инструкций) должностным лицам центра занятости по организации и обеспечению защиты информации;

включение в должностные обязанности работников центра занятости соответствующих пунктов о соблюдении порядка и правил обработки защищаемой информации и обеспечения ее безопасности, и об ответственности за нарушение

правил обращения с персональными данными и разглашение (распространение) защищаемой информации;

организация изучения работниками центра занятости законодательных и нормативных правовых актов Российской Федерации, распорядительных и организационных документов центра занятости по защите информации, порядку обработки и обеспечения безопасности персональных данных. Факт изучения требований указанных документов отражается в журнале или в листах доведения, прилагаемых к изучаемым документам;

обеспечение работников, допущенных к обработке защищаемой информации, средствами идентификации пользователей в соответствии с Положением о разрешительной системе доступа к защищаемой информации;

организация учета и хранения материальных и электронных носителей защищаемой информации, оборудование помещений, где обрабатывается защищаемая информация, и хранилищ носителей такой информации средствами, исключающими несанкционированный доступ к информации и автоматизированным информационным системам ее обработки;

ввод в эксплуатацию (приказ) объекта информатизации, предназначенного для обработки защищаемой информации;

организация аттестации объектов информатизации по требованиям безопасности информации в целях официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

4. Особенности при обработке персональных данных:

4.1. Обеспечение безопасности персональных данных в центре занятости осуществляется с учетом следующих основных положений законодательных и нормативных правовых актов, определяющих порядок получения, обработки, хранения, передачи и защиты персональных данных:

получение, обработка, хранение и обеспечение безопасности персональных данных работников центра занятости осуществляется в соответствии с положениями Трудового кодекса Российской Федерации и Федерального закона «О персональных данных»;

получение, обработка, хранение и обеспечение безопасности персональных данных субъектов, обратившихся в центр занятости за получением государственных услуг в сфере труда и занятости населения, осуществляется в соответствии с положениями Федерального закона «О персональных данных» и других нормативных правовых актов, определяющих порядок обработки персональных данных при исполнении законодательства о занятости населения в Российской Федерации;

работники центра занятости, допущенные к обработке персональных данных, принимают обязательство выполнять установленные законодательством требования по защите и неразглашении персональных данных, которое включается в текст Трудового договора (при наличии действующего Трудового договора – дополнительное соглашение);

обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки и не должны быть избыточными по отношению к заявленным целям их обработки;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

срок хранения персональных данных субъектов, обратившихся в центр занятости в поисках подходящей работы и признанных в установленном порядке безработными, содержащихся в автоматизированных информационных системах, личных делах, личных карточках и других регистрационных документах, определяется соответствующими распорядительными и нормативными документами Министерства труда и социального развития Российской Федерации и Комитета;

субъект персональных данных имеет право на получение информации о правовых основаниях и целях обработки его персональных данных, способах и сроках обработки персональных данных и сроках их хранения;

представитель центра занятости обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить установленный перечень его персональных данных, если предоставление персональных данных является обязательным в соответствии с федеральным законом;

субъект персональных данных вправе требовать от представителей центра занятости уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

передача центром занятости персональных данных сторонним организациям (третьим лицам) осуществляется только с согласия, подтвержденного личной подписью, субъекта персональных данных.

4.2. Основные положения (политика) обработки и обеспечения безопасности персональных данных в центре занятости, размещаются на стенде (в месте), доступном для ознакомления посетителей.

5. Обязанности и права должностных лиц по защите информации:

5.1. Директор центра занятости (ответственный за техническую защиту информации):

организует защиту информации в пределах компетенции центра занятости, подписывает распорядительные и утверждает организационные документы центра занятости по защите информации;

назначает (возлагает обязанности) администратора безопасности информации;

организует обучение специалистов центра занятости в области защиты информации и обеспечения безопасности персональных данных;

определяет места и порядок хранения носителей защищаемой информации, организует оборудование помещений, где обрабатывается защищаемая информация, и хранилищ носителей такой информации средствами, исключающими несанкционированный доступ к информации и автоматизированным информационным системам ее обработки;

организует контроль за соблюдением работниками центра занятости установленных требований по защите информации и правил обращения с персональными данными;

планирует потребность в финансировании мероприятий по защите информации на очередной финансовый год;

представляет центр занятости при проведении проверок в области защиты информации контрольными (надзорными) органами.

5.2. Администратор безопасности информации:

разрабатывает проекты распорядительных и организационных документов центра занятости в области защиты информации и обеспечения безопасности персональных данных;

анализирует информацию, обрабатываемую в центре занятости, условия ее обработки и хранения с целью определения потенциальных угроз безопасности информации и необходимых мер по ее защите;

организует проведение классификации автоматизированных информационных систем и отдельных (не входящих в систему) автоматизированных рабочих мест, предназначенных для обработки защищаемой информации, в соответствии с требованиями информационной безопасности и потенциальными угрозами ее безопасности;

планирует и организует выполнение мероприятий по установке сертифицированных по требованиям безопасности программных и аппаратно-программных средств защиты информации, в том числе криптографической, обеспечивающих ее техническую защиту в соответствии с результатами классификации, ведет их учет;

на основании заявок руководителей структурных подразделений центра занятости составляет Список работников, допускаемых к обработке защищаемой информации и Список работников, уполномоченных на использование средств криптографической защиты информации;

распределяет между работниками центра занятости, в соответствии с утвержденными списками, электронные средства идентификации пользователей и средства криптографической защиты информации;

формирует и распределяет системные пароли, организует и контролирует ежеквартальную смену системных и пользовательских паролей;

организует доведение до работников центра занятости положений законодательных и нормативных правовых документов Российской Федерации, распорядительных и организационных документов центра занятости по защите информации и обеспечению безопасности персональных данных;

организует учет и хранение съемных машинных носителей защищаемой информации в соответствии с требованиями нормативных документов по информационной безопасности;

организует обновление антивирусного программного обеспечения не реже одного раза в неделю;

контролирует соблюдение работниками центра занятости правил обработки защищаемой информации;

контролирует целостность средств и программного обеспечения защиты информации с целью исключения возможностей внесения несанкционированных изменений;

принимает меры по исключению возможностей подключения к защищаемым информационным системам устройств и установки в них программного обеспечения, влияющих на безопасность информации и не имеющих сертификатов соответствия требованиям по безопасности информации;

еженедельно контролирует и анализирует содержимое системных журналов защищаемых информационных систем с целью выявления и предотвращения нарушений установленных прав доступа к защищаемой информации;

организует и контролирует удаление из средств вычислительной техники, передаваемой в ремонт сторонним организациям, программного обеспечения защиты информации;

анализирует состояние системы защиты информации в центре занятости и готовит предложения по внедрению эффективных и обоснованных мер информационной безопасности;

организует заключение договоров на оказание услуг в области защиты информации со специализированными организациями, имеющими лицензию на данный вид деятельности;

готовит предложения по совершенствованию системы защиты информационных ресурсов в центре занятости и финансированию мероприятий, обеспечивающих защиту информации на очередной финансовый год период;

организует подготовку и проведение аттестации по требованиям безопасности информации автоматизированных информационных систем, предназначенных для обработки информации, подлежащей защите.

при выявлении случаев нарушения требований по защите информации или несанкционированного доступа к защищаемым сведениям незамедлительно принимает меры к их пресечению и докладывает директору центра занятости;

требует от работников центра занятости безусловного соблюдения установленной технологии обработки информации и выполнения требований по информационной безопасности;

приостанавливает эксплуатацию автоматизированных информационных систем (далее – АИС) при выявлении нарушения требований информационной безопасности до устранения причин указанных нарушений с докладом о принятых мерах директору центра занятости;

прекращает действие средств идентификации пользователей (проводить замену) и использование средств криптографической защиты информации при наличии предположений об их компрометации;

готовит доклады и отчеты по установленным формам.

5.3. Руководители структурных подразделений центра занятости:

определяют перечень работников структурного подразделения, допускаемых к обработке информации, подлежащей защите, и перечень действий с защищаемой информацией (чтение, изменение, копирование, удаление и т.п.) разрешаемых пользователю при ее обработке;

подают заявку администратору безопасности информации для включения работников структурного подразделения в Список работников, допускаемых к обработке защищаемой информации и Список работников, уполномоченных на использование средств криптографической защиты информации;

согласовывают с администратором безопасности информации установку или замену программного обеспечения на защищаемых автоматизированных системах, перемещение основных и вспомогательных технических средств в помещениях, где осуществляется обработка защищаемой информации;

обеспечивают выполнение работниками структурного подразделения установленных требований по информационной безопасности;

в случае обнаружения попыток несанкционированного доступа к защищаемой информации, предпосылок к компрометации средств идентификации пользователей и криптографической защиты информации прекращают обработку защищаемой информации и информируют об этом администратора безопасности информации;

представляют ходатайства директору центра занятости или администратору безопасности информации о назначении служебного расследования и привлечении к ответственности работников структурного подразделения, нарушивших правила обработки защищаемой информации и обеспечения ее безопасности.

5.4. Работники центра занятости обязаны:

знать и выполнять положения законодательных и нормативных правовых актов Российской Федерации, распорядительных и организационных документов центра занятости по защите информации и обеспечению безопасности персональных данных, правила обработки, хранения и передачи защищаемой информации;

проводить антивирусный контроль при каждом включении компьютера, перед использованием съемного магнитного или машинного носителя информации и по окончании его использования;

при обнаружении на машинных и магнитных носителях информации зараженных вирусами файлов провести их «лечение» и антивирусный контроль всех жестких дисков и файлов компьютера;

в случае подозрения на наличие компьютерного вируса (некорректная работа программ, искажение данных, появление графических эффектов или сообщений о системных ошибках и т.п.) провести антивирусный контроль и «лечение» всех файлов на жестких дисках компьютера;

при обнаружении вируса, не поддающегося «лечению», немедленно прекратить обработку информации, сообщить о возникшей проблеме руководителю структурного подразделения и администратору безопасности информации, дальнейшую работу начинать при твердой уверенности в отсутствии вирусов на жестких и съемных носителях информации;

обеспечить защиту обрабатываемой информации от просмотра ее посторонними лицами, в том числе работниками центра занятости, не допущенными к данной информации;

по окончании работы с информацией и базами данных осуществлять их резервное копирование;

по окончанию обработки защищаемой информации «обнулить» оперативную память компьютера путем его перезагрузки или временного выключения;

обеспечить сохранность конфигурации размещения основных и вспомогательных технических средств автоматизированного рабочего места и неизменность программного обеспечения автоматизированной информационной системы;

предоставлять защищаемую информацию сторонним организациям или третьим лицам в соответствии с правилами, установленными в десятом разделе настоящего Положения;

в случае обнаружения попыток несанкционированного доступа к защищаемой информации, предпосылок компрометации средств идентификации пользователя или криптографической защиты информации (нарушение опечатывания мест их хранения или неисправность замков на хранилищах, несанкционированное включение компьютера и т.п.) обработку защищаемой информации прекратить (не начинать) и доложить о факте предполагаемых несанкционированных действий руководителю структурного подразделения;

по окончании рабочего дня отключить все основные и вспомогательные технические средства автоматизированного рабочего места от источников электропитания, съемные машинные и магнитные носители защищаемой информации заложить на хранение в соответствии с порядком, определенным

распорядительными и организационными документами центра занятости по защите информации.

5.5. Системный администратор:

производит подключение и настройку СВТ и средств защиты информации;

выполняет работы по установке, настройке и обновлению общесистемного и прикладного программного обеспечения СВТ, в том числе антивирусного программного обеспечения;

осуществляет непосредственную настройку и проведение резервного копирования информации, её хранение и при необходимости производит восстановление утраченных или искаженных данных;

участвует в проверках выполнения требований по защите информации в центре занятости.

6. Разрешительная система доступа к защищаемой информации:

6.1. В целях разграничения прав доступа работников центра занятости к защищаемым информационным ресурсам составляется Список работников, допущенных к обработке защищаемой информации, в котором отражается перечень информационных ресурсов и права доступа к ним (создание, чтение, изменение, копирование, печать, блокирование, удаление) для каждого работника, включенного в данный список.

Список составляется администратором безопасности информации на основании заявок руководителей структурных подразделений и утверждается директором центра занятости.

При составлении заявки руководителями структурных подразделений определяются перечень информационных ресурсов и права доступа к ним работников структурного подразделения, необходимые для выполнения ими должностных обязанностей.

6.2. Доступ работников к защищаемой информации, содержащейся в автоматизированной информационной системе, осуществляется посредством ввода системных паролей или с применением других средств идентификации пользователей (ключ идентификатор и т.п.).

Пароли составляются, распределяются, учитываются в Журнале паролей и доводятся пользователям под роспись администратором безопасности информации.

Установку паролей на средства автоматизации обработки информации и их замену осуществляет системный администратор по указанию администратора безопасности информации.

6.3. Основные требования к паролям:

пароль состоит из букв в верхнем и нижнем регистрах клавиатуры, цифр и специальных символов (А, б, 5, &, *, № и т.п.);

длина пароля должна составлять не менее 6 символов;

пароль не должен содержать легко вычисляемых или распространенных сочетаний символов (имена, фамилии, даты рождения и т.п.), а также общепринятых сокращений;

при смене пароля его новое значение должно отличается от предыдущего не менее чем на четыре символа.

6.4. Смена паролей проводится не реже одного раза в 3 месяца.

В случае прекращения полномочий пользователя в связи с увольнением или переходом на другую работу смена пароля проводится по завершении последнего сеанса его работы в автоматизированной информационной системе.

В случае прекращения полномочий администратора безопасности информации Журнал паролей передается ответственному за техническую защиту информации и проводится внеплановая замена паролей на всех защищаемых средствах автоматизации обработки информации.

В случае прекращения полномочий системного администратора или компрометации пароля одного из пользователей администратором безопасности информации организуется внеплановая замена паролей на всех защищаемых средствах автоматизации обработки информации.

6.5. Администратор безопасности информации обеспечивает условия хранения Журнала паролей, исключающие доступ к парольной информации посторонних лиц.

Работники центра занятости обеспечивают сохранность парольной информации, предназначенной для их доступа в автоматизированную информационную систему.

Соблюдение прав доступа к защищаемым информационным ресурсам автоматически протоколируются операционными системами средств автоматизации обработки информации.

7. Антивирусный контроль:

7.1. Антивирусный контроль осуществляется в целях предотвращения воздействий на программное обеспечение средств автоматизации и обрабатываемую информацию программных вирусов, приводящих к нарушению работоспособности программ автоматизированной информационной системы и искажению, блокированию или утрате защищаемой информации.

7.2. Антивирусное программное обеспечение, устанавливаемое на средствах автоматизации, предназначенных для обработки защищаемой информации, должно быть сертифицировано по требованиям безопасности информации.

7.3. Установка, настройка и обновление антивирусного программного обеспечения осуществляются системным администратором по указанию администратора безопасности информации.

7.4. Антивирусный контроль информации на жестких дисках автоматизированной информационной системы проводится при каждом включении и выключении компьютера его пользователем.

7.5. Антивирусный контроль съемных магнитных и машинных носителей информации проводится пользователем перед началом и по окончании работы с ними в автоматизированной информационной системе.

7.6. Администратор безопасности информации организует обновление антивирусного программного обеспечения на всех средствах автоматизации, предназначенных для обработки защищаемой информации, не реже одного раза в неделю.

7.7. Руководители структурных подразделений центра занятости осуществляют повседневный контроль выполнения работниками требований по антивирусному контролю.

8. Резервное копирование и восстановление информации:

8.1. Резервное копирование защищаемой информации осуществляется в целях обеспечения ее целостности и достоверности при возникновении неисправностей технических средств, ошибок и сбоев в работе программного обеспечения,

воздействии программных вирусов и в результате воздействия на информацию непреднамеренных ошибок пользователей.

8.2. Перечень информационных ресурсов, подлежащих обязательному резервному копированию, сроки и порядок хранения резервных копий информации определяются директором центра занятости на основании обоснованных предложений администратора безопасности информации и руководителей структурных подразделений с учетом положений законодательных и нормативных правовых актов о персональных данных.

8.3. Резервное копирование проводится на жесткие магнитные диски серверов и (или) съемные носители информации по окончании обработки защищаемой информации в течении рабочего дня.

8.4. Порядок резервного копирования информации на жесткие диски серверов определяется администратором безопасности информации.

8.5. Повседневный контроль за выполнением работниками центра занятости требований по резервному копированию защищаемой информации возлагается на руководителей соответствующих структурных подразделений.

8.6. Восстановление заблокированной, искаженной или утраченной информации за счет ее резервных копий проводится с разрешения администратора безопасности информации после полного устранения причин, приведших к негативному воздействию на информацию.

9. Обновление программного обеспечения:

9.1. Установка и обновление программного обеспечения средств автоматизации обработки защищаемой информации проводится с разрешения директора центра занятости (ответственного за техническую защиту информации) на основании нормативных документов, предписывающих применение данного программного продукта, или предложений администратора безопасности информации и руководителей структурных подразделений центра занятости.

9.2. Устанавливаемое программное обеспечение или обновленные версии ранее установленного программного обеспечения должны иметь соответствующие лицензии.

9.3. Программное обеспечение, используемое при обработке защищаемой информации, должно быть сертифицировано по требованиям безопасности.

9.4. Установка и обновление элементов программного обеспечения проводится системным администратором или представителями разработчика данного программного продукта без допуска их к защищаемой информации.

9.5. Все работы по установке и обновлению программного обеспечения на средствах автоматизации, предназначенных для обработки защищаемой информации, проводятся под контролем администратора безопасности информации.

9.6. Установка и обновление программного обеспечения защищенных средств автоматизации обработки информации, путем их подключения к информационно-телекоммуникационной сети «Интернет» ЗАПРЕЩАЕТСЯ.

10. Действия при компрометации средств криптографической защиты информации и идентификации пользователей:

10.1. Компрометация средств криптографической защиты информации (далее – СКЗИ) или средств идентификации пользователей, обеспечивающих доступ к защищаемой информации, содержащейся в автоматизированной информационной системе относится к основным нарушениям системы защиты информации.

10.2. Действия должностных лиц при компрометации средств криптографической защиты информации и идентификации пользователей:

10.2.1. Работник центра занятости, являющийся пользователем средств криптографической защиты информации и (или) идентификации пользователей, обязан незамедлительно прекратить обработку защищаемой информации и поставить в известность руководителя структурного подразделения и администратора безопасности информации в случаях:

компрометации паролей доступа к объектам информатизации или возникновения предположений об их компрометации;

утраты носителей ключевой информации СКЗИ;

утраты носителей ключевой информации СКЗИ и последующего их обнаружения;

нарушения целостности печатей на тубусах или других хранилищах носителей ключевой информации СКЗИ;

доступа к паролям или к ключевой информации посторонних лиц;

обнаружения несанкционированных изменений в конфигурации программных или аппаратных средств защиты информации;

обнаружения сбоев в работе программных и аппаратно-программных средств защиты информации.

10.2.2. Администратор безопасности информации:

в случае компрометации паролей доступа к информации защищаемой автоматизированной информационной системы или возникновения предположений об их компрометации незамедлительно организует замену действующих паролей, изучает и анализирует причины, приведшие к компрометации, и организует устранение указанных причин, о факте компрометации и принятых мерах по обеспечению защиты информации докладывает ответственному за техническую защиту информации;

в случае обнаружения несанкционированных изменений в конфигурации программных или аппаратных средств защиты информации и сбоев в работе программных и аппаратно-программных средств защиты информации немедленно прекращает доступ к информационным системам, защищаемым данными средствами, проводит служебное расследование по данным фактам и организует устранение причин указанных нарушений, о результатах служебного расследования и принятых мерах по обеспечению защиты информации докладывает ответственному за техническую защиту информации;

в случае компрометации или признаков компрометации ключа электронной подписи немедленно докладывает об этом ответственному за техническую защиту информации и организует уведомление о данном факте Удостоверяющего центра с целью приостановки действия сертификата скомпрометированного ключа. Организует служебное расследование по факту компрометации ключа электронной подписи и устранение причин способствовавших компрометации. Готовит заявку на возобновление действия сертификата или организует получение нового сертификата ключа электронной подписи.

10.2.3. Директор центра занятости в период приостановки действия сертификата скомпрометированного ключа электронной подписи или до получения нового сертификата организует обмен документами посредством бумажных, магнитных и машинных носителей информации, о чем уведомляет адресатов (абонентов) в день приостановки действия ключа электронной подписи.

11. Предоставление информации, подлежащей защите, сторонним организациям:

11.1. Информация, подлежащая защите (персональные данные), предоставляется сторонним организациям (третьим лицам) на основании письменных запросов которые должны быть исполнены за подписью руководителя (заместителя руководителя) организации и содержать обоснование необходимости получения конкретной информации со ссылками на положения законодательных и нормативных правовых актов.

11.2. Подготовка информации для передачи сторонним организациям (третьим лицам) осуществляется по письменному указанию директора центра занятости и предоставляется за его подписью или подписью должностного лица, исполняющего его обязанности.

При этом ответ на запрос не должен содержать избыточных сведений либо не запрашиваемой информации.

11.3. При передаче экземпляров (копий) документов центра занятости, содержащих защищаемую информацию, на обороте оригинала документа проставляется отметка о количестве переданных экземпляров (копий) документов, а также адресатов, которым они направлены.

11.4. Размножение документов, содержащих информацию с пометкой «Для служебного пользования», присланных другими организациями, без письменного разрешения этих организаций ЗАПРЕЩАЕТСЯ.

11.5. Документы, содержащие защищаемую информацию, пересылаются заказными почтовыми отправлениями или курьерами.

Документ, подтверждающий получение носителя такой информации адресатом (уведомление о вручении, реестр, отметка на экземпляре и т.п.), подшивается вместе с экземпляром исходящего документа, предназначенным в дело.

11.6. Информация, подлежащая защите, передается по открытым каналам связи с применением средств криптографической защиты информации.

12. Хранение носителей защищаемой информации и средств криптографической защиты информации:

Места и порядок хранения бумажных и электронных носителей защищаемой информации, средств криптографической защиты информации и идентификации пользователей устанавливаются директором центра занятости с соблюдением положений законодательных и нормативных правовых документов и с учетом следующих основных требований:

расположение, оборудование и организация режима допуска в помещения, предназначенные для хранения носителей защищаемой информации и средств криптографической защиты информации (далее – спецпомещения) должны исключать возможность неконтролируемого пребывания в них посторонних лиц и просмотра посторонними лицами ведущихся там работ;

спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное их закрытие в нерабочее время. Один экземпляр ключа находится у работника, ответственного за данное помещение, запасные экземпляры ключей хранятся в сейфе (запираемом и опечатываемом ящике стола или тумбочки) директора центра занятости;

окна спецпомещений, расположенных на первом или последнем этаже здания, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в них посторонних лиц, необходимо оборудовать металлическими

решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения;

по окончании рабочего дня спецпомещения должны быть закрыты и опечатаны, ключи в опечатанном виде сданы под расписку в соответствующем журнале службе охраны, печати, предназначенные для опечатывания спецпомещений, должны находиться у работников, ответственных за эти помещения;

в случае, когда охрана здания или помещений центра занятости осуществляется путем постановки на сигнализацию, подключенную к пульту охранной организации (отсутствие физической охраны), ключи от спецпомещений в опечатанном виде закладываются в надежно запираемое хранилище (сейф, шкаф, ящик рабочего стола или тумбочки), определяемое директором центра занятости;

аппаратно-программные средства криптографической защиты информации, электронные носители ключевой информации (ключи электронной подписи, ключи идентификации пользователей, компакт – диски и дискеты с программами шифрования защищаемой информации в прикладном программном обеспечении, поставляемом взаимодействующими организациями и т.п.), техническая документация и сертификаты соответствия требованиям по безопасности информации к ним подлежат поэкземплярному учету администратором безопасности информации в соответствующем журнале;

аппаратно-программные средства криптографической защиты информации должны быть оборудованы средствами контроля за их вскрытием (опечатывание, опломбирование), место опечатывания, опломбирования должно обеспечить постоянный визуальный контроль целостности печати (пломбы);

электронные носители ключевой информации хранятся в опечатанном виде (тубусы и т.п.) в целях исключения бесконтрольного доступа к ним посторонних лиц и их компрометации, ответственность за обеспечение хранения, исключающего их компрометацию, возлагается на работников центра занятости, допущенных к использованию указанных электронных носителей ключевой информации.

13. Планирование защиты информации:

13.1. План основных мероприятий по защите информации на очередной год составляется до 30 декабря текущего года администратором безопасности информации на основании:

законодательных и нормативных правовых актов Российской Федерации по защите информации и обеспечению безопасности персональных данных;

методических рекомендаций и указаний Комитета по защите информации и обеспечению безопасности персональных данных;

анализа состояния системы защиты информации и эффективности ранее принятых мер;

рекомендаций надзорных и контролирующих органов по результатам проверок.

13.2. План основных мероприятий по защите информации утверждается директором центра занятости.

14. Контроль состояния защиты информации:

13.1. Контроль состояния и эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения

несанкционированного доступа к информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности информационных систем.

14.2. Контроль заключается в проверке выполнения положений законодательных и нормативных правовых актов по защите информации, обоснованности и эффективности, принятых мер информационной безопасности.

14.3. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации, проводится администратором безопасности информации и руководителями структурных подразделений, в ведении которых находятся объекты информатизации и защищаемая информация.

14.4. Периодический плановый контроль осуществляется представителями ФСТЭК России, ФСБ России, Роскомнадзора России и Прокуратуры Российской Федерации по планам данных надзорных органов.

Допуск представителей указанных органов, кроме представителей Прокуратуры Российской Федерации, для проведения контроля осуществляется по предъявлению служебного удостоверения и предписания на право проверки, подписанного руководителем (заместителем руководителя) соответствующего органа.

Представители Прокуратуры Российской Федерации допускаются к проверке в соответствии с положениями Федерального закона «О прокуратуре Российской Федерации».

14.5. Администратор безопасности информации обязан присутствовать при всех проверках по вопросам защиты информации, проводимых контрольными (надзорными) органами.

14.6. При выявлении недостатков в организации защиты информации и обеспечении безопасности персональных данных, не устраненных в ходе проверки, администратором безопасности информации в десятидневный срок составляется план устранения недостатков, который утверждается директором центра занятости.

15. Ответственность за нарушение требований по защите информации

За нарушение установленного законодательными и нормативными правовыми актами порядка сбора, обработки, хранения, передачи и распространения информации, подлежащей защите, должностные лица несут ответственность в соответствии с законодательством Российской Федерации:

15.1. Трудовой кодекс Российской Федерации.

статья 81. Трудовой договор может быть расторгнут работодателем в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника;

статья 90. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

15.2. Кодекс Российской Федерации об административных правонарушениях:

статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей;

статья 13.14. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей, на должностных лиц - от четырех тысяч до пяти тысяч рублей.

15.3. Федеральный закон «Об информации, информационных технологиях и о защите информации».

Статья 17, часть 2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Администратор
безопасности информации _____ (подпись) Васильева Н.В. (расшифровка подписи)