Утверждено:

Приказом №___ от _____20___ г.
Генерального директора АО «АИЖК ЯО»
Ямнюка Я.Б.
Разработано:
Заместителем генерального директора АО «АИЖК ЯО»
Кузнецовым В.Ю.

ПОЛОЖЕНИЕ

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных АО «Агентство ипотечного жилищного кредитования Ярославской области»

1. Общие положения.

1.1. Данное «Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением 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», приказом ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 13 февраля 2008 года и методическими рекомендациями ФСТЭК России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.2. Допуск пользователей для работы на компьютере осуществляется на основании разрешения руководителя структурного подразделения (отдела) АО «АИЖК ЯО» в соответствии со списком лиц, допущенных к работе в ИСПДн в соответствии со списком ролей ИСПДн, выявленным в ходе проведения последней Внутренней проверки.

2.3. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для записи и хранения информации, содержащей ПДн, разрешается использовать только учтенные носители информации.

2.4. Пользователь несет ответственность за правильность включения и выключения компьютера, входа в систему и все действия при работе в ИСПДн.

2.5. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю в соответствии с Инструкцией по порядку формирования, распределения и применения паролей.

2.6. При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютере. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения и Инструкцией по защите от компьютерных вирусов.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютере;
- хранить в тайне свой пароль (пароли). В соответствии с п.п. 8.5., 8.6. данного Положения и с установленной периодичностью менять свой пароль (пароли);
- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- выполнять требования антивирусной защиты в полном объеме.

Немедленно известить администратора безопасности ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при их обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках компьютера или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данной защищенному компьютеру;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию компьютера, выхода из строя или неустойчивого функционирования узлов компьютера или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютере технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю компьютера категорически **ЗАПРЕЩАЕТСЯ**:

- использовать компоненты программного и аппаратного обеспечения компьютера в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения компьютера;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным и/или без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы исключить возможность визуального считывания информации.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации.

Резервирование и восстановление работоспособности технических средств и программного обеспечения баз данных и средств защиты информации в АО «АИЖК ЯО» определяется «Порядком резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации в информационной системе АО «АИЖК ЯО».

4. Порядок контроля ИСПДн, приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях учреждения/организации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

- выявление демаскирующих признаков объектов ИСПДн;

- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн АО «АИЖК ЯО»;

- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах АО «АИЖК ЯО» и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации.

4.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);

- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- эффективность применения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

4.5. Основными видами технического контроля на объектах, являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации ответственный по безопасности ИСПДн докладывает директору для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются в виде записей в соответствующих журналах.

4.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию директора проводится служебное расследование.

Расследование осуществляется постоянно действующей Комиссией по вопросам организации и ведения мероприятий по работе с конфиденциальной информацией и защите персональных данных АО «АИЖК ЯО» (далее - Комиссия). Комиссия обязана установить, имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования директор принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, силами штатных сотрудников осуществляющих обслуживание баз данных, технических и программных средств с участием администратора безопасности ИСПДн в соответствии с утвержденным АО «АИЖК ЯО» планом или по предварительному с ним согласованию.

4.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год.

4.10. Обследование объектов информатизации и связи проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств, и систем требованиям по защите информации.

4.11. В ходе обследования проверяется:

- соответствие категории обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

- соблюдение организационно-режимных требований защищаемых помещений;

- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

- наличие электробытовой, радио и телевизионной аппаратуры, и устройств непромышленного изготовления (пультов связи, устройств вызова и оповещения, усилителей,

генераторов и других вспомогательных технических средств, и систем), которые могут способствовать возникновению каналов утечки информации;

- выполнение требований предписаний на эксплуатацию на основные технические средства и системы по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;

- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в техническом паспорте;

- выполнение требований по защите автоматизированных систем от несанкционированного доступа;

- выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры, оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

- вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

- проверить качество установки стеклопакетов оконных приемов;

- провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры).

4.13. Периодический контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России в соответствии с действующим законодательством Российской Федерации. Доступ представителя указанного федерального органа исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, справки о допуске, а также предписания установленной формы на право проведения проверки.

5. Порядок обучения персонала практике работы в ИСПДн.

5.1. Обучение практике и методике в ИСПДн должно быть непрерывным, систематическим, разделенным по категориям, при этом наибольшее внимание следует уделять практике работы пользователя с ИСПДн.

5.2. Обучение по методике делятся на:

- совещания;
- обучающие занятия, семинары;
- инструктажи;
- методическая помощь и практические занятия на месте.

5.3. Совещания, обучающие занятия и семинары проводятся согласно плану АО «АИЖК ЯО» по организации защиты информации на год.

5.4. Инструктажи, методическая помощь и практические занятия по вопросам обеспечения безопасности ИСПДн должны проводиться в ходе плановых, периодических и внезапных проверок состояния обеспечения безопасности ИСПДн на местах.

5.6. Первичные инструктажи проводятся администратором безопасности ИСПДн с пользователями ИСПДн при поступлении сотрудника на работу в АО «АИЖК ЯО», где происходит обработка конфиденциальной информации в ИСПДн.

5.7. Ответственным за организацию обучения и оказание методической помощи АО «АИЖК ЯО» является администратор безопасности ИСПДн.

5.8. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты организаций лицензиатов, а также органов по аттестации объектов ИСПДн.

5.9. К работе в ИСПДн допускаются только сотрудники, прошедшие инструктаж обеспечения безопасности в ИСПДн.

6. Порядок проверки электронного журнала обращений к ИСПДн.

6.1. Настоящий раздел Положения определяет порядок проверки электронного журнала обращений к ИСПДн.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к конфиденциальной информации в ИСПДн.

6.3. Право проверки электронного журнала обращений имеют:

- Директор;
- администратор безопасности ИСПДн.

6.4. В ИСПДн, где установлены средства защиты информации (далее – СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлены случай НСД к информации конфиденциального характера то вступает в силу п.п. 4.7., 4.8. данного Положения.

7. Правила антивирусной защиты.

Правила антивирусной защиты в информационных системах АО «АИЖК ЯО» содержатся в «Инструкции по защите от компьютерных вирусов в информационных системах АО «АИЖК ЯО».

8. Правила парольной защиты.

Правила, регламентирующие организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями, определяются в «Инструкции по порядку формирования, распределения и применения паролей в информационных системах персональных данных АО «АИЖК ЯО».

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн.

Порядок регламентирующий обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн определяется в «Положении об обновлении общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн в АО «АИЖК ЯО».

10. Порядок контроля соблюдения условий использования средств защиты информации.

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

10.2. Технические средства защиты информации являются важным компонентом обеспечения безопасности ПДн.

10.3. Порядок работы с техническими СЗИ определен в соответствующих Инструкциях к СЗИ, в Руководстве по настройке и использованию СЗИ, обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратору (ответственному) по безопасности ИСПДн АО «АИЖК ЯО».

10.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- Директор.

- Ответственному за организации защиты персональных данных (администратор по безопасности).

10.5. Пользователю ИСПДн категорически запрещается:

- обработка конфиденциальной информации с отключенными СЗИ;

- менять настройки СЗИ.

10.6. Ответственному за организации защиты персональных данных ИСПДн запрещается менять настройки программно-аппаратных СЗИ предустановленные сотрудником организации выполняющей работы по аттестации в ходе настройки системы обеспечения безопасности ПДн при аттестации ИСПДн.

10.7. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5. то вступает в силу п.п. 4.7., 4.8. данного Положения.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения.

11.1. Настоящее Положение устанавливает порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн.

11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения определяется руководителем структурного подразделения (отдела) по согласованию с Ответственным за организации защиты персональных данных АО «АИЖК ЯО».

11.3. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

11.4. При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержится конфиденциальная информация сдаются руководителю структурного подразделения (отдела) для хранения в опечатываемом сейфе (металлическом шкафу).

11.5. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт. О происшествии немедленно сообщается директору и администратору по безопасности ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия руководителя структурного подразделения и администратора безопасности по ИСПДн в помещение никто не допускается.

11.6. Руководитель структурного подразделения и администратор по безопасности ИСПДн организуют проверку АРМ, ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации, о чём докладывается непосредственно директору АО «АИЖК ЯО».

11.7. В соответствии с требованиями данного Положения при обработке конфиденциальной информации в ИСПДн необходимо исключить возможность неконтролируемого пребывания посторонних лиц в пределах границ контролируемой зоны ИСПДн.

12. Заключительные положения.

12.1. Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих конфиденциальную информацию в ИСПДн в АО «АИЖК ЯО».

12.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.