УТВЕРЖДАЮ
Председатель кооператива
ЖКС «Энергетик»
_____ Ю.Ю. Золотов
«09» января 2018 г

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
информационных систем персональных данных кооператива ЖКС «Энергетик»

2018 г.

1. Общие положения

1.1 Настоящий документ разработан в соответствие с нормативными документами в области защиты персональных данных и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) Кооператив ЖКС «Энергетик» (далее – Кооператив).

1.2 Администратор информационной безопасности (далее – АИБ) назначается приказом председателя Кооператива.

1.3 АИБ осуществляет контроль выполнения требований по обеспечению безопасности персональных данных при их обработке в ИСПДн дополнительно к своим непосредственным обязанностям.

1.4 АИБ имеет неограниченные права доступа к ресурсам ИСПДн.

1.5 АИБ осуществляет общее руководство и контроль за обеспечением информационной безопасности пользователями ИСПДн и обслуживающим персоналом.

1.6 АИБ осуществляет методическое руководство по обеспечению безопасности персональных данных в ИСПДн.

1.7 АИБ имеет право вносить предложения по изменению и дополнению данной инструкции и «Инструкции пользователя ИСПДн».

1.8 Изменения и дополнения к данной инструкции утверждаются в установленном порядке.

2. Требования к администратору информационной безопасности

2.1 АИБ, не ознакомленный с данной инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПДн не допускается.

2.2 АИБ **ОБЯЗАН**:

2.2.1 знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите персональных данных;

2.2.2 знать состав основных и вспомогательных технических систем, и средств (далее - ОТСС и ВТСС), установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

2.2.3 осуществлять установку, настройку и сопровождение ПО, средств защиты информации;

2.2.4 участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;

2.2.5 производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от несанкционированного доступа (далее - НСД) и сопровождать их в процессе эксплуатации, при этом реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

2.2.6 участвовать в приемке новых программных средств;

2.2.7 периодически тестировать функции СЗИ, особенно при изменении программной среды и полномочий исполнителей;

2.2.8 восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

2.2.9 контролировать физическую сохранность средств и оборудования ИСПДн;

2.2.10 обеспечивать постоянный контроль за выполнением сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

2.2.11 контролировать работу пользователей в сетях общего пользования и (или) международного обмена;

2.2.12 периодически, согласно утвержденному плану, производить проверку работоспособности аппаратных и программных средств защиты информации (СЗИ);

2.2.13 немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (ОТСС и ВТСС), СЗИ, системного и прикладного программного обеспечения (ПО);

2.2.14 немедленно ставить в известность руководство обо всех неисправностях аппаратно-программных средств ИСПДн.

2.2.15 немедленно сообщать ответственному по защите информации в ИСПДн об имеющих место попытках несанкционированного доступа (НСД) к информации и техническим средствам вычислительной техники, а также принимать необходимые меры по устранению нарушений:

- установить причины, по которым стал возможным НСД;
- установить личность нарушителя;
- установить последствия, к которым привел НСД;
- зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;
- провести инструктаж с пользователями ИСПДн по выполнению требований информационной безопасности.

2.2.16 обеспечивать соблюдение сотрудниками, допущенными для обслуживания объектов информатизации, утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств ИСПДн;

2.2.17 обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания элементов ИСПДн и отправке их в ремонт (контролировать изъятие жестких магнитных носителей с составлением соответствующего акта);

2.2.18 присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

2.2.19 контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям, вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения);

2.2.20 осуществлять контроль за порядком создания, учета, хранения и использования резервных и архивных копий массивов данных;

2.2.21 проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам ИСПДн;

2.2.22 проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и системами защиты информации;

2.2.23 производить периодическое обновление информационных баз антивирусного программного обеспечения;

2.2.24 проводить анализ системного журнала для выявления попыток НСД к защищаемым ресурсам не реже одного раза в месяц.

2.2.25 принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий;

2.2.26 Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними специалистами на территории Учреждения.

2.3 АИБ **ИМЕЕТ ПРАВО**:

2.3.1 проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки информации;

2.3.2 разрабатывать все планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ОТСС, СЗИ, ВТСС.

2.3.3 требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите персональных данных в ИСПДн;

2.3.4 инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

2.3.5 обращаться к ответственному по защите информации в ИСПДн с требованием прекращения работы в ИСПДн при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;

2.3.6 требовать от пользователя изменения его пароля.

3. Порядок работы администратора с ресурсами ИСПДн

3.1 Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн

АИБ присваивает пользователям ИСПДн идентификационные данные и права доступа к соответствующим ресурсам ИСПДн и контролирует их соответствие. При этом должны выполняться следующие требования:

- АИБ разрабатывает политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
- АИБ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует выполнение пользователем парольной политики;
- изменение учетных данных пользователя производится по требованию руководителя подразделения, согласованному с АИБ, а также периодически по утвержденному плану и в случае увольнения сотрудника;
- АИБ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АИБ обязан потребовать у пользователя изменения пароля.

3.2 Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ).

АИБ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить. В случае сбоя программных СЗИ АИБ обязан работы прекратить, но в случае производственной необходимости – отключить ПО СЗИ и лично контролировать процесс проведение работ пользователя.

3.3 Антивирусная защита ресурсов ИСПДн.

АИБ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры средств антивирусной защиты;
- контролирует работоспособность средств антивирусной защиты;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений средств антивирусной защиты;
- имеет право на проведение внеплановой проверки на присутствие вирусов;
- периодически (не реже одного раза в неделю) обновляет антивирусные базы данных, а также исполняемые модули антивирусной программы.

3.4 Хранение дистрибутивов программного обеспечения СЗИ.

АИБ должен хранить дистрибутивы программного обеспечения СЗИ, установленного в ИСПДн в месте, исключающем доступ посторонних лиц.

3.5 Резервное копирование и восстановление информации.

В соответствии с технологическим процессом, а также по требованию пользователей ИСПДн, АИБ производит резервное копирование и восстановление системного и прикладного ПО, а также документов, содержащих персональные данные. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе технических средств ИСПДн или отчуждаемых машинных носителей;
- допускается обоснованное внеплановое резервное копирование информации по инициативе АИБ, если это не нарушает технологию обработки информации;
- резервные копии с операционной системой и другим системным и прикладным ПО хранятся у администратора информационной безопасности;

– в процессе и по мере устранения сбоев АИБ производит восстановление информации и СЗИ;

– все операции по резервированию и восстановлению информации должны быть зарегистрированы.

3.6 Вывод ресурсов ИСПДн из эксплуатации.

При невозможности ремонта различных ресурсов ИСПДн АИБ обязан:

– физически уничтожать любые МН (Машинные Носители информации), независимо от содержащейся на них информации;

– остальные комплектующие могут быть использованы за пределами ИСПДн;

4. Ответственность администратора информационной безопасности

4.1. На АИБ возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации.

4.2. АИБ несет ответственность в соответствии с действующим законодательством за разглашение сведений ограниченного распространения ставших известными ему по роду работы.