УТВЕРЖДЕНО
Приказом генерального директора
Общества с ограниченной ответственностью «Техновек»
От 25.08.2022 года № 1/ПНд

Громова В.В.

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «Техновек»

1. ТЕРМИНЫ

В настоящем документе могут использоваться следующие термины и их определения:

Безопасность информации [данных] - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействии на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ к информации - возможность получения информации и ее использования.

Защита информации (ЗИ) - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Примечание - Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в

виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно - вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и(или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Цель защиты информации - заранее намеченный результат защиты информации.

Примечание - Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящее Положение об организации и проведению работ по обеспечению безопасности персональных данных (далее - Положение) утверждается руководителем ООО «Техновек» (далее – Общество/Организация) и определяет направления, мероприятия, порядок организации, процедуры и правила проведения работ по обеспечению безопасности и защите персональных данных при их обработке в информационных системах ООО «Техновек» (далее – защищаемая информация).

2.2. Минимальная периодичность пересмотра настоящего положения – 1 год, максимальная периодичность пересмотра – 2 года.

2.3. Перечень обрабатываемых Обществом персональных данных приведен в Положении об обработке и защите персональных данных ООО «Техновек».

2.4. Целями настоящего Положения являются:

- выполнение требований нормативных документов Российской Федерации, связанных с персональными данными;
- защита прав и свобод граждан РФ при обработке их персональных данных в Обществе;
- обеспечение исключения неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования и распространения ПДн;
- обеспечение исключения неправомерного или случайного доступа, уничтожения, блокирования, копирования материальных носителей персональных данных и технических средств их обработки;
- обеспечение конфиденциальности, целостности, доступности ПДн;
- предотвращение утечек ПДн;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- снижение уровня регуляторных рисков в отношении Общества;
- обеспечение исключения иных неправомерных действий в отношении персональных данных.

2.5. Настоящее Положение разработано с учетом положений следующих законодательных, нормативно-правовых актов и локальных нормативных актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года.
- Постановление Правительства Российской Федерации от 15 сентября 2008 года No 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 17 ноября 2007 года No 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Совместный приказ от 13 февраля 2008 года ФСТЭК России No 55, ФСБ России No 86 и Министерства информационных технологий и связи No20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

- Положение об обработке и защите персональных данных ООО «Техновек»;
- Актуального Приказа руководителя ООО «Техновек» об определении уровня защищенности персональных данных.

2.6. Настоящее положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения информационной безопасности;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение угроз безопасности информации;
- координации деятельности структурных подразделений Общества при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению информационной безопасности;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения информационной безопасности в ИСПДн.

2.7. К основным задачам в области обеспечения безопасности ПДн относится:

- определение новых ИСПДн;
- инвентаризация и управление изменениями в составе и структуре ИСПДн;
- сбор согласий на обработку ПДн с субъектов ПДн;
- разработка и актуализация Перечня персональных данных, обрабатываемых в Обществе;
- контроль целей обработки ПДн, состава обрабатываемых ПДн целям обработки;
- уничтожение ПДн;
- оптимизация информационных процессов обработки ПДн;
- управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;
- взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
- классификация ИСПДн;
- разработка (актуализация) документации на систему защиты ПДн;
- выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
- сертификация применяемых средств защиты информации;
- эксплуатация системы защиты ПДн в соответствии с документацией на нее;
- контроль уровня защищенности ПДн;
- обучение персонала по вопросам защиты ПДн;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к обработке ПДн; взаимодействие с регуляторными органами по вопросам защиты ПДн;
- актуализация и подача уведомлений в Уполномоченный орган по защите прав субъектов ПДн;
- реагирование на нештатные ситуации, расследование нештатных ситуаций, возникающих при обработке ПДн;
- получение лицензий ФСТЭК России и ФСБ России в области защиты ПДн; контроль лояльности администраторов ИСПДн.

2.8. Принципы и требования по обеспечению безопасности персональных данных распространяются:

- на все возможные формы существования информации, такие как:
– физические поля (электрические, акустические, электромагнитные, оптические и т.п.);
- носители на бумажной, магнитной, оптической и иной основе.
- на все возможные форматы представления персональных данных, такие как:
– документы;
– голос;
– изображения;
– файлы;
– почтовые сообщения;
– базы данных;
– записи базы данных;
– другие информационные массивы.

2.9. Положения настоящего Положения обязательны к исполнению для всех работников ООО «Техновек», пользователей информационных систем ООО «Техновек» (далее - Пользователи), которые участвуют в обработке ПДн, как автоматизированной, так и не автоматизированной, либо в организации такой обработки.

2.10. Категорирование ПДн и классификация ИСПДн проведены Обществом в соответствии с «Порядком проведения классификации информационных систем персональных данных» (утвержденным Совместным приказом от 13 февраля 2008 года ФСТЭК России No55, ФСБ России No86 и Мининформсвязи России No20). Процесс категорирования ПДн и классификации ИСПДн явился основой для определения требований к уровню защиты ПДн, определенном в Акте комиссии Общества.

2.11. Принципы и требования по организации работы с персональными данными распространяются на все возможные носители информации, такие как:
- Бумажные носители;
- Электронные носители;
- Электрические сигналы в проводнике;
- акустические колебания и т.п.;

и на все возможные форматы представления персональных данных, такие как:
- документы;
- голос;
- файлы;
- почтовые сообщения;
- базы данных;
- записи базы данных;
- другие информационные массивы.

3. Технологический процесс обработки информации

3.1. Технологический процесс обработки информации полностью описываются комплексом процедур автоматизированной обработки данных обусловленных функциональными возможностями технических и программных средств ИСПДн.

3.2. Этапы автоматизированной обработки данных в ИСПДн полностью описываются следующими процедурами:

- ввод данных в ИСПДн;
- формализация и сортировка данных;
- запись данных;
- чтение данных;
- копирование/перенос данных;
- модификация и преобразование данных;
- архивация данных;
- удаление данных;
- транспортировка данных по внутренним каналам связи;
- вывод данных из ИСПДн.

3.3. Ввод информации в ИСПДн осуществляется пользователями ИСПДн следующими способами:

3.3.1. ввод информации с клавиатуры рабочей станции;

3.3.2. путем копирования и (или) переноса ее с отчуждаемых носителей информации (Flash- накопители, CD, DVD-CD, внешние HDD), при этом в ИСПДн не допускается использование не учтенных машинных носителей информации;

3.3.3. перемещение информации в безопасное облачное хранилище.

3.4. Формализация, модификация, преобразование, запись, чтение и сортировка данных осуществляется с использованием функционала используемого программного обеспечения.

3.5. Программное средство обработки данных выбирается в зависимости от формата представления данных. Эксплуатация функций программных средств должна осуществляться в строгом соответствии с эксплуатационной документацией на данное ПО.

3.6. Для модификации, уничтожения, копирования и (или) переноса информации пользователь должен обратиться к защищаемому ресурсу и после проверки его полномочий подсистемой выполнить необходимые действия.

3.7. Копирование/перенос, удаление и транспортировка данных по внутренним каналам связи осуществляется с использованием средств операционной системы.

3.8. Архивация данных осуществляется с использованием как штатных средств операционной системы, так и с использованием прикладного программного обеспечения.

3.9. Вывод информации из ИСПДн производится следующим образом:

3.9.1. на печатающие устройства;

3.9.2. на предварительно учтенные бумажные носители;

3.9.3. на предварительно учтенные машинные носители информации (оптические диски, флэш-накопители);

3.9.4. на безопасные облачные хранилища.

3.10. Копирование информации допускается:

3.10.1. на учтенные машинные носители информации (оптические диски, флэш-накопители);

3.10.2. на безопасные облачные хранилища.

3.11. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).
3.12. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели, обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4. СИСТЕМА ЗАЩИТЫ ПДн

4.1. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

4.2. В целях обеспечения уровня защищенности персональных данных при их обработке в ИСПДн, ООО «Техновек», а также его работники, обязано организовывать и соблюдать следующие требования:

4.2.1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

4.2.2. обеспечение сохранности носителей персональных данных;

4.2.3. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

4.2.4. назначение должностного лица (работника) ответственного за обеспечение безопасности персональных данных в ИСПДн.

4.3. В обществе должно проводиться регулярное обучение (не реже одного раза в год) работников по вопросам, связанным с защитой ПДн.

4.4. При допуске к ПДн необходимо руководствоваться Приказом о допуске к обработке ПДн. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

4.5. В локальных актах Общества, в отношении сотрудников, допущенных к обработке ПДн, должен указываться перечень разрешенных операций с персональными данными. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

4.6. Перечень помещений, в которых разрешена работа с ресурсами ИСПДн, расположены технические средства ИСПДн, перечень лиц, допущенных в эти помещения, перечень устройств (стационарных, мобильных, портативных), используемых в процессе обработки ПДн определяется руководителем ООО «Техновек» и фиксируется в Приказе.

4.7. Контролируемая зона, перечень технических средств ИСПДн, а также лиц, допущенных в контролируемую зону, определяется Приказом, утверждаемом руководителем ООО «Техновек». Администратор безопасности обеспечивает актуальность перечня, а также организует охрану контролируемой зоны в рабочее и нерабочее время.

4.8. Помещения, в которых осуществляется обработка защищаемой информации, оборудованы охранной и пожарной сигнализациями, а также прочными дверьми с механическими замками. Ключи от помещений выдаются и находятся на ответственном хранении у сотрудников, которым необходим доступ в эти помещения для выполнения своих служебных (должностных) обязанностей. При покидании помещения и при отсутствии в нем других лиц, допущенных в это помещение, сотрудник обязан проследить, чтобы в помещении не было посторонних лиц, и закрыть помещение на ключ.

4.9. При завершении рабочего дня сотрудники отделений обязаны выполнить следующие мероприятия:

- убрать документы с персональными данными в шкафы, сейфы или запирающиеся на ключ шкафы;
- выключить установленным порядком вычислительную технику и оргтехнику;
- закрыть окна;
- выключить электроприборы;
- выключить свет;
- закрыть входную дверь на замок;
- ключ от входной двери в помещение сотрудник отделения сохраняет у себя.

4.10. Перед началом рабочего дня помещения снимаются с охраны. После окончания рабочего дня, помещения устанавливаются под охрану.

4.11. Нахождение посторонних лиц (в том числе в помещениях, в которых осуществляется обработка защищаемой информации, допускается только в присутствии сотрудников, работающих в данном помещении и при условии соблюдения правил ограничения доступа к обрабатываемой информации. При проведении таких работ работники отделения обязаны принять меры по исключению ознакомления работников сторонних организаций с персональными данными.

4.12. Запрещается оставлять помещения, в которых ведется обработка персональных данных, без присмотра работников, имеющих допуск в помещения, где ведется обработка персональных данных.

4.13. Запрещается оставлять без присмотра находящихся в помещении, в которых ведется обработка персональных данных, посторонних лиц, а также, работников, не имеющих допуск в помещения, в которых ведется обработка персональных данных.

4.14. В состав ИСПДн входят стационарные ПК. В ИСПДн реализована многопользовательская модель доступа без разграничения прав. ИСПДн предназначена для обработки персональных данных работников и иных категорий персональных данных. АРМ из ИСПДн имеет выход в сети общего пользования.

4.15. Обработка информации, содержащей персональные данные, допускается в ИСПДн успешно прошедших аттестацию и предназначенных для этих целей.

4.16. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ООО «Техновек», допущенному к работе с ресурсами ИСПДн присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать.

4.17. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИПСДн запрещено.

4.18. Парольная защита при работе на ИСПДн осуществляется с целью предотвращения НСД к защищаемой информации.

4.19. Личные пароли доступа к ИСПДн, СЗИ от НСД, первично назначаются пользователям Администратором ИБ при формировании персонального идентификатора, при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее шести символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования ИСПДн, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны путем анализа информации об ответственном исполнителе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 123456 и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4 позициях;
- в числе символов пароля могут присутствовать латинские буквы в верхнем и нижнем регистрах, цифры;
- не использовать ранее использовавшиеся пароли.

4.20. Лица, использующие пароли, обязаны четко знать и строго выполнять требования настоящего Положения и других руководящих документов по использованию парольной защиты, а также своевременно сообщать Администратору ИБ обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

4.21. При организации парольной защиты запрещается: записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПК, на обратной стороне клавиатуры и т.п.); хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги; сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

4.22. Защита с применением паролей других программно – технических средств и программных продуктов осуществляется, при их наличии, в соответствии с эксплуатационной документацией на эти средства.

4.23. Полная плановая смена паролей в ИСПДн проводится регулярно Администратором ИБ ИСПДн и пользователями, не реже одного раза в 6 (шесть) месяцев.

4.24. Компрометация действующих паролей является нештатной ситуацией, о чем должен быть уведомлено лицо, назначенное ответственным за обработку и защиту ПДн.

4.25. Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия должностных лиц, приведшие к получению его пароля лицами, не имеющими на то права.

4.26. Скомпрометированные пароли и связанные с ними персональные идентификаторы пользователей незамедлительно выводятся из действия.

4.27. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

4.28. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

4.29. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

4.30. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

4.31. Лицо ответственное за ИБ:
4.31.1. при необходимости проводит инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты;
4.31.2. осуществляет контроль за своевременным обновлением антивирусных программных средств;
4.31.3. осуществляет периодический контроль за соблюдением пользователями ПК требований настоящей Инструкции.

4.32. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник Общества самостоятельно или вместе с администратором ИБ ИСПДн должен провести внеочередной антивирусный контроль ПК. При необходимости он должен пригласить Администратора ИБ ИСПДн для определения факта наличия или отсутствия компьютерного вируса.

4.33. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Общества обязаны:

4.33.1. приостановить работу;

4.33.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя Общества, Администратора ИБ ИСПДн, а также иных сотрудников, использующих эти файлы в работе;

4.33.3. провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта пригласить Администратора ИБ ИСПДн);

4.33.4. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору ИБ ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

4.33.5. по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИБ ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

4.34. Неавтоматизированная и автоматизированная обработки ПДн в электроном виде осуществляются на внешних электронных носителях информации и в облачном хранилище.

4.35. Материальными носителя ПДн являются: бумажные носители, несъемные магнитные (жесткие диски и т.д.), схемные магнитооптические (дискеты и т.д.), съемные оптические носители (CD\DVD и т.д.), а также съемные и несъмные носителя на основе флеш-памяти.

4.36. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, выдаёт съёмные носители пользователям-работникам Общества или сотруднику по гражданско-правовому договору, допущенным к обработке персональных данных Приказом, в случаях производственной необходимости под роспись.

4.37. Каждый носитель данных, применяемый при обработке ПДн должен иметь грф «Конфиденциально». Учетный номер и гриф «Конфиденциально» наносятся на носитель информации или его корпус. Если невозможно непосредственно машинный носитель данных, то маркируется упаковка, В которой хранится носитель. В этом случае учетный номер записывается также на носитель любым возможным способом.

4.38. Пользователям, получившим съёмные носители персональных данных под подпись, запрещается передавать их третьим лицам.

4.39. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, изымает съёмные носители персональных данных при увольнении пользователя.

4.40. Если машинный носитель был сломан, его необходимо вывести из эксплуатации по причине сдачи в ремонт, а затем заново ввести в эксплуатацию.

4.41. Машинные носители данных после удаления с ним ПДн с учета не снимаются и хранятся в порядке, предусмотренном настоящей Политикой. В последующем эти носители могут использоваться для записи ПДн. Если носители непригодны для дальнейшего использования, они подлежат уничтожению по акту.

4.42. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

4.43. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов), если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

4.44. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.

4.45. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных, сообщают об этом ответственному за обеспечение безопасности персональных данных.

4.46. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению.

4.47. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.

4.48. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учета съёмных носителей персональных данных:

4.48.1. учётный номер, размещённый на этикетке на съёмном носителе персональных данных;

4.48.2. тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD диск);

4.48.3. серийный или инвентарный номер съёмного носителя;

4.48.4. место хранения (номер запираемого шкафа или сейфа, номер помещения);

4.48.5. дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя;

4.48.6. подпись.

4.49. При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

4.50. При уходе в отпуск, служебной командировке и в иных случаях длительного отсутствия сотрудника на своем рабочем месте он обязан передать носители, содержащие ПДн, лицу, на которое локальным актом возложено исполнение его трудовых обязанностей.

4.51. В случае обработки ПДн с помощью сервисов облачного хранения, Общество создает учетную запись пользователя на платформе провайдера, имеющего аппаратные ресурсы на территории Российской Федерации, а также сервис которого соответствует требованиям Федерального закона №152 «О защите персональных данных» от 27.06.2006 г., «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утверждённым Постановлением Правительства РФ №1119 от 01.11.2012 года, «Состав и содержание технических и организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённым Приказом ФСТЭК №21 от 18.02.2013 года,
4.52. ISO, GDPR, PCI DSS, РПО и ГОСТ Р 57580, и обеспечивает, как минимум, первый уровень защищенности ПДн (УЗ-1).

4.53. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, предоставляет данные для аутентификации и авторизации пользования на облачной платформы (логин и пароль либо пин-кож) только тем работникам Общества или сотрудникам по гражданско-правовому договору, которые допущены к обработке персональных данных Приказом Общества.

4.54. Провайдер отвечает за физическую безопасность и отказоустойчивость платформы, защищает сеть, собирает и анализирует события безопасности гипервизоров и других компонентов инфраструктуры. Провайдер хранит пользовательские данные в зашифрованном виде; защита данных при передаче по каналам интернета обеспечивается протоколом TLS.

4.55. Трансграничная передача персональных данных третьим лицам осуществляется на основании соответствующего договора, содержащего требования конфиденциальности персональных данных и их защиты в соответствии с законодательством РФ.

4.56. В случае достижения цели обработки персональных данных Общество обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

4.57. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Общество обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

4.58. Уничтожение документов, содержащих персональные данные, производится: в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

4.59. Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов.

4.60. Уничтожение ПДн может быть осуществлено способами в зависимости от типа носителя информации:
4.60.1. Физическое уничтожение носителя (уничтожение через шредерование, сжигание);
4.60.2. Уничтожение информации с носителя (удаление папки, перезапись CD\DVD носителя);
4.60.3. Уничтожение с сервиса облачного хранения (удаление папки).
4.60.4. подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске компьютера, удаляются средствами операционной системы компьютера с последующим «очищением корзины»
4.60.5. уничтожение осуществляется по акту.

5. Общий порядок действий при возникновении нештатных ситуаций

5.1. В настоящем документе под нештатной ситуацией понимается происшествие, связанное сосбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же с вероятностью потери защищаемой информации.

5.2. К нештатным ситуациям относятся следующие ситуации:
5.2.1. сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т. п.);
5.2.2. отключение электричества;
5.2.3. сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);
5.2.4. выход из строя сервера;

5.2.5. потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);
5.2.6. обнаружен вирус;
5.2.7. обнаружена утечка информации (взлом учетной записи пользователя);
5.2.8. обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);
5.2.9. взлом системы (web-сервера, файл-сервера и др.) или несанкционированный доступ;
5.2.10. попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);
5.2.11. компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.).

5.3. При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность руководителя Общества.

5.4. Ответственный сотрудник проводит предварительный анализ ситуации, принимает необходимые в зависимости от ситуации действия и меры в отношении нештатной ситуации, описанные в настоящей Политике:
5.4.1. проводит анализ на наличие потерь и/или разрушения данных;
5.4.2. Проверяет работоспособность оборудования;
5.4.3. исправляет ошибку при сбое программного обеспечения;
5.4.4. восстанавливает ПО и данные последней резервной копии;
5.4.5. проводит антивирусную проверку;
5.4.6. локализует вирус с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера;
5.4.7. после успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса;
5.4.8. после ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ПЭВМ Общества с применением обновленных антивирусных баз;
5.4.9. проводит анализ защищенности систем, принимает меры по устранению уязвимостей и предотвращению их возникновения;
5.4.10. временно отключает сервер от сети для проверки на вирусы и троянских закладок;
5.4.11. производит смену паролей и принимает необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.).

5.5. При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

5.6. Ответственный работник Общества периодически, не реже 1 раза в год, проводит анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

6. Ответственность лиц, допущенных к обработке ПДн в Обществе

6.1. Руководитель, разрешающий доступ сотрудника к персональным данным, несет персональную ответственность за данное разрешение.

6.2. Каждый работник Общества или сотрудник, привлеченный по гражданско-правовому договору, получающий для работы персональные данные иных субъектов, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

6.3. Лица, виновные в нарушении норм, регламентирующих получение, обработку и защиту персональных данных, в том числе и обрабатываемых в автоматизированной информационной системе Общества несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

6.4. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Обществе организовывается проведение плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27 июля 2006 г. No152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), принятым в соответствии с ним нормативным правовым актам и локальным актам Общества (далее - проверка).

6.5. Проверки проводятся в Обществе на основании ежегодного плана или на основании поступившего в Общество письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

6.6. Проведение внеплановой проверки организуется в течение 5 рабочих дней с момента поступления обращения.

6.7. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.