Министерство здравоохранения Омской области
Бюджетное учреждение здравоохранения Омской области
«КЛИНИЧЕСКИЙ ДИАГНОСТИЧЕСКИЙ ЦЕНТР»
(БУЗОО «КДЦ»)

ПРИКАЗ

22 апреля 2019 г. № 29 адм

г. Омск

Об утверждении политики обработки персональных данных

В целях соблюдения требований Федерального закона от 27 июля 2016г. № 152–ФЗ «О персональных данных» и других нормативно - правовых актов и нормативно-методических документов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности персональных данных,

п р и к а з ы в а ю:

1. Утвердить:

1.1. Политику обработки персональных данных в БУЗОО «КДЦ» (Приложение 1 к данному Приказу).

1.2. Инструкцию пользователя в части обеспечения безопасности персональных данных при возникновении внештатных ситуаций (Приложение 2 к данному Приказу).

2. Ведущему документоведу отдела документационного обеспечения ознакомить всех заинтересованных должностных лиц под роспись в трехдневный срок с момента регистрации и разместить электронную копию документа в электронной сети БУЗОО « КДЦ».

3. Заместителю главного врача по ОМР обеспечить размещение Политики обработки персональных данных в сети Интернет на официальном сайте БУЗОО «КДЦ».

4. Контроль за исполнением Приказа возложить на заместителя главного врача по организационно - методической работе.

Главный врач Орлова Н.И.

Исп.Бодрова Т.В.
2-17

Приложение 1
к Приказу
от 22.04.2019 № 29 адм

ПОЛИТИКА
обработки персональных данных в БУЗОО «КДЦ»

1 Общие положения

1.1. Настоящая Политика обработки персональных данных (далее - Политика) БУЗОО «КДЦ» ИНН 5504001891, 644024, РФ, Омская обл., г. Омск, ул. Ильинская, 9 (далее - Оператор) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», иными федеральными законами и нормативно-правовыми актами.

1.2. Политика разработана с целью обеспечения защиты прав и свобод субъектов персональных данных (далее - ПДн) при обработке их ПДн.

1.3. Настоящая Политика распространяется на персональные данные, полученные как до, так и после ее утверждения.

1.4. В дополнение к настоящей Политике Оператор может выпускать дополнительные нормативные документы, регламентирующие защиту и порядок обработки персональных данных.

1.5. Действие настоящего документа распространяется на все процессы Оператора, в рамках которых осуществляется обработка персональных данных, а также на подразделения, принимающие участие в указанных процессах.

1.6. Основные понятия

персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

2 Цели обработки ПДн

2.1. ПДн обрабатываются Оператором в следующих целях:

1) Обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей, в частности:

- выполнение требований законодательства в сфере труда и налогообложения;
- ведение текущего бухгалтерского и налогового учёта;
- формирование, изготовление и своевременная подача бухгалтерской, налоговой и статистической отчётности.

2) Обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн (работник или клиент), в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

3) Обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну, а также работники, в служебные обязанности которых входит обработка

первичной медицинской документации, содержащей сведения, составляющие врачебную тайну.

4) Обработка ПДн необходима для защиты жизни, здоровья, или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно.

3.Правовое основание обработки ПДн

3.1. Обработка ПДн осуществляется на основе следующих федеральных законов и нормативно-правовых актов:

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральный закон РФ от 24 июля 2009 года № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;
- Федеральный закон от 01 апреля 1996 года № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 6 декабря 2011 года № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон РФ от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 02 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»
- Законом РФ от 07 февраля 1992 года № 2300-1 «О защите прав потребителей»;
- Постановление Правительства Российской Федерации от 4 октября 2012 года № 1006 г. «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;
- Гражданский Кодекс РФ (ст. 152);
- Трудовой Кодекс РФ от 30 декабря 2001 года № 197-ФЗ (ст. 65, ст. 86-90);
- постановление Правления ПФР от 31 июля 2006 года № 192 п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению»;
- постановление Государственного комитета Российской Федерации по статистике от 5 января 2004 года № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- приказ ФНС от 17 ноября 2010 года № ММВ-7-3/611 «Об утверждении формы сведений о доходах физических лиц и рекомендации по ее заполнению, формата сведений о доходах физических лиц в электронном виде, справочников»;

– приказ Министерства здравоохранения и социального развития Российской Федерации № 441н от 02 мая 2012 года «Об утверждении Порядка выдачи медицинскими организациями справок и медицинских заключений»;

– Устав БУЗОО «КДЦ»;

– Лицензия Министерства здравоохранения Омской области № ЛО-55-01-002389 ОТ 27.08.2018 г. «На осуществление медицинской деятельности».

4. Перечень действий с ПДн

4.1. При обработке ПДн оператор осуществляет следующие действия с ПДн:

- блокирование;
- запись;
- извлечение;
- использование;
- накопление;
- обезличивание;
- передачу (распространение, предоставление, доступ);
- сбор;
- систематизация;
- удаление;
- уничтожение ПДн
- уточнение (обновление, изменение);
- хранение.

4.2. Медицинская документация постоянно дополняется новыми данными обследования, данными изменения состояния здоровья пациента и результатами медицинских вмешательств. Все данные, полученные из различных источников, используются, в соответствии с законодательством РФ, исключительно в интересах пациента, для уточнения диагноза его заболевания и повышения эффективности проводимой терапии.

4.3. Уточнение предполагает изменение, обновление сведений, отражающих изменение состояние пациента в процессе выполнения медицинского вмешательства. Поскольку процесс оказания медицинской помощи динамичный, постоянно меняющийся, то и эти данные по мере их поступления уточняются (обновляются, изменяются), что позволяет менять тактику лечения, использовать более эффективные методы терапии, выполнять более информативные методы диагностики.

4.4. При обработке персональных данных Оператор обеспечивает точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры (обеспечивает их принятие) по удалению или уточнению неполных или неточных персональных данных.

4.5. Хранение ПДн должно осуществляться в форме, позволяющей идентифицировать субъекта ПДн, не дольше, чем этого требуют цели обработки

ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого является субъект ПДн.

4.6. Уничтожение или выдача медицинской документации по просьбе (заявлению) клиента не допускается, более того, как указывалось ранее, документация должна храниться в архиве учреждения в течение строго определенного срока, установленного законодательными актами. Учитывая указанные требования действующего законодательства РФ и ведомственные нормативно-правовые акты, первичные медицинские документы должны быть оформлены и сданы в архив (без права дальнейшей обработки) в течение 3 (трех) рабочих дней, со дня даты поступления заявления клиента.

5.Состав обрабатываемых ПДн

5.1. Обработке Оператором подлежат ПДн следующих субъектов ПДн:

5.1.1. ПДн работников в составе:

- фамилия, имя, отчество;
- год рождения;
- место рождения;
- гражданство;
- трудовая деятельность;
- сведения о детях (имя, фамилия, отчество, год рождения);
- сведения о премировании;
- телефон;
- начисления заработной платы;
- паспортные данные или данные иного документа, удостоверяющего личность;
- аттестация;
- квалификационный экзамен;
- отпуска;
- ИНН;
- номер страхового свидетельства государственного пенсионного страхования;
- домашний адрес;
- фотография.

5.1.2. ПДн клиентов в составе:

- Фамилия, имя, отчество;
- дата рождения;
- возраст;
- пол;
- СНИЛС;
- номер телефона;
- документ удостоверяющий личность (тип документа, серия, номер дата выдачи, кем выдан);

– гражданство;
– социальный статус;
– место работы;
– место учебы;
– должность;
– адрес прописки;
– адрес проживания;
– полис ОМС (серия и номер, дата действия);
– номер договора;
– ЛПУ прописки;
– полис ДМС (серия и номер, дата действия);
– сведения об оплате;
– группа крови;
– резус-принадлежность;
– побочное действие лекарств (непереносимость);
– кем направлен больной (название лечебного учреждения);
– диагноз направившего учреждения;
– диагноз при поступлении;
– дата установления диагноза;
– диагноз заключительный клинический;
– госпитализирован в данном году по поводу данного заболевания (впервые, повторно);
– хирургические операции, методы обезболивания и послеоперационные осложнения;
– виды лечения;
– данные о выданных листках нетрудоспособности;
– исход заболевания;
– трудоспособность(восстановлена полностью, снижена, временно утрачена, стойко утрачена в связи с данным заболеванием);
– патоморфологический диагноз;
– срок беременности;
– номер пробирки для анализа;
– дата забора материала;
– дата исследования;
– результат исследования;
– результат дополнительного исследования.
– масса;
– рост;
– инвалидность (нет\с рождения\приобретенная);
– группа здоровья;
– рекомендации по дальнейшему лечению.

5.1.3. ПДн контрагентов в составе:

– фамилия, имя, отчество;
– занимаемая должность;
– паспортные данные или данные иного документа, удостоверяющего личность;
– домашний адрес;
– юридический адрес;
– ИНН;
– КПП;
– телефон;
– E-mail;
– банковские реквизиты.

6.Обработка ПДн

6.1. Основанием для обработки ПДн субъекта, не являющегося работником Оператора или лицом, заключившим с Оператором договор, является согласие в письменной форме субъекта ПДн на обработку его ПДн.

6.2. Обработка ПДн осуществляется с согласия субъекта ПДн (работники, клиенты, контрагенты) на обработку его ПДн.

6.3. Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточными по отношению к заявленным целям обработки.

6.4. ПДн клиентов (пациенты или их законные представители) и контрагентов обрабатываются Оператором с использованием средств автоматизации и без использования таких средств, с фиксацией ПДн на материальном носителе (бумажные документы).

6.5. ПДн работников обрабатываются Оператором с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, и без использования таких средств, с фиксацией ПДн на материальном носителе (бумажные документы).

6.6. В случае отказа субъекта персональных данных предоставить свои персональные данные Оператор в обязательном порядке разъясняет субъекту юридические последствия такого отказа.

6.7. Поручение обработки персональных данных третьему лицу осуществляется только на основании договора, заключенного между Оператором и третьим лицом, либо ином основании, предусмотренном действующим законодательством, при наличии согласия субъекта персональных данных, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

7.Обеспечение защиты ПДн при их обработке Оператором

7.1.Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным

законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

7.2.Оператор самостоятельно определил состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации», Приказом ФСТЭК от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами. К таким мерам относятся:

– назначение Оператором ответственного за организацию обработки ПДн;

– издание Оператором документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности ПДн;

– осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике Оператора в отношении обработки ПДн, локальным актам оператора;

– определение оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– ознакомление работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

7.3.Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.Право субъекта ПДн (работник, клиент, контрагент) на доступ к его ПДн

8.1.Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными,

устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2.Сведения предоставляются субъекту ПДн или его законному представителю оператором при обращении либо при получении запроса субъекта ПДн или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.3.Оператор вправе отказать субъекту ПДн в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

8.4.Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, а именно:

– подтверждение факта обработки ПДн Оператором;

– правовые основания и цели обработки ПДн;

– цели и применяемые Оператором способы обработки ПДн;

– наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;

– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом «О Персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу.

8.5.Если субъект ПДн считает, что Оператор осуществляет обработку его ПДн с нарушением требований Федерального закона «О Персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Оператора в уполномоченном органе по защите прав субъектов ПДн.

8.6.Субъект ПДн имеет право отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

8.7.Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8.8.Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской федерации.

9.Обязанности Оператора

В соответствии с требованиями Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ Оператор обязан:

9.1.Предоставлять субъекту персональных данных по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить мотивированный отказ от предоставления такой информации в срок, предусмотренный Федеральным законом «О персональных данных».

9.2.По требованию субъекта персональных данных уточнять обрабатываемые персональные данные, блокировать или удалять, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

9.3.Уведомлять субъекта персональных данных об обработке персональных данных в том случае, если персональные данные были получены не от субъекта персональных данных. Исключение составляют следующие случаи:

– субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим Оператором;

– персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника.

10.Ответственный за организацию обработки ПДн

10.1.Ответственный за организацию обработки ПДн в БУЗОО «КДЦ» назначается приказом главного врача.

10.2.За дополнительными разъяснениями субъектам ПДн необходимо обращаться к ответственному за организацию обработки ПДн.

11.Заключительные положения

11.1.Внесение изменений в настоящую Политику должно производиться при изменении действующего законодательства Российской Федерации, по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

11.2.Настоящая Политика и все изменения к ней утверждаются и вводятся в действие приказом главного врача БУЗОО «КДЦ».

11.3.Ответственность должностных лиц БУЗОО «КДЦ», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.

Приложение 2
к Приказу
от 22.04.2019 № 29 осн

ИНСТРУКЦИЯ
пользователя в части обеспечения безопасности персональных данных при возникновении внештатных ситуаций

1. Назначение и область действия

1.1. Настоящая инструкция определяет порядок действий пользователей при возникновении внештатных ситуаций при работе с персональными данными в информационных системах персональных данных (далее – ИСПДн) БУЗОО «КДЦ», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций, и по реагированию на внештатные ситуации, связанные с работой в ИСПДн.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Пользователями ИСПДн (далее – Пользователь) являются сотрудники, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки защищаемой информации и имеющие доступ к аппаратным средствам, программному обеспечению и данным ИСПДн согласно перечню лиц, которым необходим доступ к персональным данным, обрабатываемым в ИСПДн, для выполнения своих служебных обязанностей.

1.4. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Общий порядок действий при возникновении внештатных ситуаций

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

К внештатным ситуациям относятся следующие ситуации:

- сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т. п.);
- отключение электричества;
- сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);
- выход из строя сервера;
- потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);
- обнаружен вирус;
- обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);
- взлом системы (web-сервера, файл-сервера и др.) или несанкционированный доступ;
- попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);
- компрометация ключей (утеря носителя ключевой информации (Rutoken, E-token и т. п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр

носителя информации посторонним лицом или подозрение, что данные факты имели место, взлом учётной записи пользователя);

– компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);

– физическое повреждение ЛВС или ПЭВМ (не включается ПК, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);

– стихийное бедствие;

– иные внештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИСПДн и возможность потери защищаемой информации, и названные таковыми пользователем ИСПДн или администратором безопасности ИСПДн.

2.2. При возникновении внештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность администратора безопасности. В случае если поставить в известность администратора не представляется возможным (администратор безопасности отсутствует на рабочем месте), пользователем, обнаружившим нештатную ситуацию, составляется служебная записка в свободной форме с описанием нештатной ситуации, и передается руководителю подразделения.

2.3. Администратор безопасности ИСПДн проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного начальника для определения дальнейших действий. Здесь и далее – в случае отсутствия администратора безопасности, все действия и меры в отношении нештатной ситуации, описанные в настоящей инструкции, выполняет сотрудник отдела АСУ, временно назначенный начальником отдела, либо сам начальник отдела АСУ.

2.4. При необходимости, проводится служебное расследование по факту возникновения внештатной ситуации и выяснению ее причин.

3. Особенности действий при возникновении наиболее распространенных внештатных ситуаций

3.1. Сбой программного обеспечения.

Администратор безопасности ИСПДн, совместно с сотрудником, у которого произошла внештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, разработчику ПО направляется информационное сообщение с сопроводительными материалами о возникшей ситуации.

3.2. Отключение электричества.

Администратор безопасности ИСПДн, совместно с сотрудником, у которого произошла внештатная ситуация, проводят анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

3.3. Сбой в локальной вычислительной сети (ЛВС).

Администратор безопасности ИСПДн проводит анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

3.4. Выход из строя сервера.

Администратор безопасности ИСПДн проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы ИСПДн. При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

3.5. Потеря данных.

При обнаружении потери данных Администратор безопасности ИСПДн проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.

3.6. Обнаружен вирус.

При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области сотрудником. Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты», инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ПЭВМ, входящих в состав ИСПДн с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ПЭВМ (ЛВС).

3.7. Обнаружена утечка информации.

При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн и ответственный за организацию обработки ПДн. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

3.8. Взлом системы (Web-сервера, файл-сервера и др.) или несанкционированный доступ (НСД).

При обнаружении взлома сервера ставится в известность Администратор безопасности ИСПДн. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянские закладки. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ПЭВМ. По факту взлома сервера проводится служебное расследование.

3.9. Попытка несанкционированного доступа (НСД).

При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн и ответственный за организацию обработки ПДн. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД (данный журнал ведется автоматизированным способом средствами защиты информации от несанкционированного доступа). По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

3.10. Компрометация ключей.

При обнаружении утечки информации ставится в известность Администратор безопасности и начальник подразделения. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

3.11. Компрометация пароля.

При обнаружении утечки информации ставится в известность Администратор безопасности и начальник подразделяния. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба. При необходимости, проводится служебное расследование.

3.12. Физическое повреждение ЛВС или ПЭВМ.

Ставится в известность Администратор безопасности ИСПДн. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

3.13. Стихийное бедствие.

При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в учреждении.

4. Меры против возникновения внештатных ситуаций

4.1. Администратором безопасности ИСПДн периодически, не реже 1 раза в год, должен проводиться анализ зарегистрированных внештатных ситуаций для выработки мероприятий по их предотвращению.

4.2. В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований организационно-распорядительных документов и инструкций по эксплуатации оборудования и ПО в части обеспечения безопасности информации.

4.3. Рекомендации по предотвращению некоторых типичных нештатных ситуаций:

– сбой программного обеспечения – применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ПЭВМ.

– отключение электричества – использовать источники бесперебойного питания на критически важных технологических участках организации.

– сбой ЛВС – обеспечивать бесперебойную работу ЛВС путем применения надежных сетевых технологий и резервных систем.

– выход из строя серверов – применять надежные программно-технические средства, допускать к работе с серверным оборудованием только квалифицированных специалистов.

– потеря данных – периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации; проводить с администраторами информационной безопасности (и сотрудниками) разъяснительные и обучающие собрания; обеспечить резервное копирование данных.

– обнаружение вируса – соблюдать требования «Инструкции по организации антивирусной защиты».

– утечка информации – применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию системы защиты информации.

– попытка несанкционированного доступа (НСД) – по возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен несанкционированный доступ, с оповещением Администратора безопасности о попытках НСД.

– компрометация паролей – соблюдать требования «Инструкции по организации парольной защиты».

– физическое повреждение ЛВС или ПЭВМ – физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним.

– стихийное бедствие – проводить обучающие собрания и тренировки персонала по вопросам гражданской обороны.

4.4. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения, что включает:
  - пожарные сигнализации и системы пожаротушения;
  - системы вентиляции и кондиционирования;
  - системы резервного питания.
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.
- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;

4.5. Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты информации) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

4.6. Ответственные за реагирование сотрудники ознакомляют всех сотрудников организации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

4.7. Должно быть проведено обучение должностных лиц Организации, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

4.8. Должностные лица должны получить базовые знания в следующих областях:

- пожаротушение;
- защита материальных и информационных ресурсов;
- выключение оборудования, электричества, водоснабжения.

4.9. Администратор безопасности и системный администратор должен быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

4.10. Навыки и знания должностных лиц по реагированию на внештатные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении внештатных ситуаций.