УТВЕРЖДЕНО

Приказом <НАЗВАНИЕ ДОЛЖНОСТИ>
<НАЗВАНИЕ ОРГАНИЗАЦИИ>

<ФИО>

№____ от «___» _____ 20 ___г.

ИНСТРУКЦИЯ

администратору информационной безопасности
<НАЗВАНИЕ ОРГАНИЗАЦИИ>

1 Введение

1.1 Данная инструкция определяет круг задач, основные права и обязанности администратора информационной безопасности <ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ> (далее по тексту — <НАЗВАНИЕ ОРГАНИЗАЦИИ>).

2 Общие положения

2.1 Назначение на должность администратора информационной безопасности, закрепление за данным лицом определенных полномочий и обязанностей производится приказом <ДОЛЖНОСТЬ> <НАЗВАНИЕ ОРГАНИЗАЦИИ>.

2.2 В своей деятельности администратор информационной безопасности руководствуется требованиями действующего законодательства Российской Федерации и внутренних документов <НАЗВАНИЕ ОРГАНИЗАЦИИ> по вопросам защиты информации, обеспечивает их выполнение в <НАЗВАНИЕ ОРГАНИЗАЦИИ>.

2.3 Администратор информационной безопасности непосредственно подчиняется <ДОЛЖНОСТЬ> <НАЗВАНИЕ ОРГАНИЗАЦИИ> и, помимо обязанностей, закрепленных настоящей Инструкцией, исполняет его указания и распоряжения в рамках выполнения своих основных задач.

3 Основные задачи администратора информационной безопасности

3.1 Основными задачами администратора информационной безопасности являются:

– ведение и актуализация перечня работников <НАЗВАНИЕ ОРГАНИЗАЦИИ>, имеющих доступ к персональным данным (далее по тексту – ПДн), обрабатываемым в <НАЗВАНИЕ ОРГАНИЗАЦИИ>;

– оценка угроз безопасности ПДн, обрабатываемых в информационных системах персональных данных (далее по тексту – ИСПДн) <НАЗВАНИЕ ОРГАНИЗАЦИИ>, и их источников;

– участие в выборе методов и способов защиты ПДн, обрабатываемых в ИСПДн, формирование требований по обеспечению безопасности ПДн с помощью технических методов защиты;

– участие в проектировании системы защиты персональных данных (далее по тексту – СЗПДн) и внедрении средств защиты информации, взаимодействие с подрядными организациями, привлеченными для выполнения данных работ;

– мониторинг функционирования средств защиты информации;

– участие в реагировании на инциденты информационной безопасности, связанные с нарушением заданных характеристик безопасности ПДн, обрабатываемых в ИСПДн;

– обеспечение соблюдения требований по безопасности информации при эксплуатации технических средств, а также при выводе технических средств или их элементов из эксплуатации, в том числе при передаче в ремонт.

4 Обязанности администратора информационной безопасности

4.1 На администратора информационной безопасности возлагаются обязанности по разработке и поддержанию в актуальном состоянии матрицы доступа к защищаемым информационным (программным) ресурсам <НАЗВАНИЕ ОРГАНИЗАЦИИ>, включающей в себя:

– перечень ИСПДн <НАЗВАНИЕ ОРГАНИЗАЦИИ>;

– перечень защищаемых информационных (программных) ресурсов <НАЗВАНИЕ ОРГАНИЗАЦИИ>;

– перечень сотрудников <НАЗВАНИЕ ОРГАНИЗАЦИИ>, допущенных к самостоятельной работе на рабочих местах ИСПДн;

– перечень сторонних лиц, имеющих доступ к ИСПДн <НАЗВАНИЕ ОРГАНИЗАЦИИ> в целях обработки ПДн;

– перечень лиц, допущенных к обслуживанию ИСПДн <НАЗВАНИЕ ОРГАНИЗАЦИИ>;

– права различных категорий лиц, допущенных к работе на рабочих местах ИСПДн, в отношении защищаемых информационных (программных) ресурсов.

4.2 На основании матрицы доступа администратор информационной безопасности поручает администратору ИСПДн (системному администратору) создавать учетные записи пользователей ИСПДн и назначать им соответствующие права в отношении защищаемых ресурсов, генерировать необходимую для доступа к ИСПДн аутентификационную (парольную) и ключевую информацию, подготавливать при необходимости материальные носители аутентификационной и ключевой информации.

4.3 Администратор информационной безопасности проводит инструктаж работников <НАЗВАНИЕ ОРГАНИЗАЦИИ> по вопросам обеспечения безопасности ПДн, обрабатываемых в ИСПДн, при предоставлении им возможности доступа к ИСПДн и выдает под роспись пользователям ИСПДн материальные носители аутентификационной и ключевой информации (в случае их использования).

4.4 Администратору информационной безопасности запрещается разрешать доступ к ПДн, обрабатываемым в ИСПДн, работникам <НАЗВАНИЕ ОРГАНИЗАЦИИ>, не включенным в перечень лиц, доступ к ПДн которым необходим для выполнения служебных (трудовых) обязанностей.

4.5 Администратор информационной безопасности несет ответственность за назначение лицам минимально необходимого им для выполнения служебных обязанностей набора прав в отношении защищаемых информационных (программных) ресурсов.

4.6 Длина паролей, выбираемых администратором информационной безопасности, должна быть не менее 12 символов. В качестве пароля должна быть выбрана последовательность букв верхнего и нижнего регистра с обязательным включением цифр и (или) специальных символов. Категорически запрещается использование в качестве пароля легко угадываемых последовательностей символов (идентификатор пользователя, его фамилия, имя или отчество, номер телефона, имена родственников, последовательно расположенные на стандартной клавиатуре символы, табельный номер и т. п.). Запрещается использование в качестве паролей слов распространенных мировых языков независимо от раскладки клавиатуры, в которой они набираются. Рекомендуется наряду с английскими буквами использовать буквы русского алфавита (с переключением набора символов на клавиатуре).

4.7 Пароли администратора информационной безопасности должны быть уникальными и не должны совпадать с другими паролями администратора информационной безопасности, в частности, с паролями электронной почты, программ обмена мгновенными сообщениями и др.

4.8 Максимальный срок использования паролей администратора информационной безопасности – 4 месяца.

4.9 Администратору информационной безопасности запрещается хранить пароли в записанном виде. За нарушение данного правила администратор информационной безопасности может быть привлечен к дисциплинарной ответственности.

4.10 Хранение администратором информационной безопасности паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе главного врача <НАЗВАНИЕ ОРГАНИЗАЦИИ> в опечатанном личной печатью пенале (конверте). При нарушении целостности печати или утрате бумажного носителя пароли считаются скомпрометированными и подлежат немедленной смене.

4.11 На администратора информационной безопасности возлагаются обязанности по разработке модели угроз безопасности ПДн, обрабатываемых в ИСПДн <НАЗВАНИЕ ОРГАНИЗАЦИИ>, в соответствии с требованиями действующих нормативно-методических документов. Разрабатываемая администратором информационной безопасность модель угроз безопасности ПДн, обрабатываемых в ИСПДн, должна включать:

– описание возможных источников угроз безопасности ПДн, обрабатываемых в ИСПДн;

– оценку возможности реализации угроз безопасности ПДн с учетом принятых в <НАЗВАНИЕ ОРГАНИЗАЦИИ> мер защиты, условий функционирования ИСПДн, других объективных и субъективных факторов;

– оценку вреда, который может быть причинен субъекту ПДн в случае реализации угрозы безопасности ПДн.

4.12 Администратор информационной безопасности ежегодно осуществляет пересмотр (актуализацию) модели угроз безопасности ПДн, обрабатываемых в ИС-

ПДн. Кроме того, актуализация модели угроз безопасности ПДн должна осуществляться в случае:

– ввода в эксплуатацию новой ИСПДн;

– внесения существенных изменений в технологический процесс обработки ПДн в ИСПДн <НАЗВАНИЕ ОРГАНИЗАЦИИ>, в условия функционирования ИСПДн;

– реализации мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, существенно влияющих на оценку возможности реализации угроз безопасности ПДн, обрабатываемых в ИСПДн.

4.13 Администратор информационной безопасности ведет учет применяемых средств защиты информации, эксплуатационной и технической документации к ним по установленной форме.

4.14 Администратор информационной безопасности обязан обеспечить надежное хранение дистрибутивов к средствам защиты информации, документации к ним, документации на СЗПДн в целом.

4.15 Администратор информационной безопасности регулярно проводит контроль соблюдения условий эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией. Нарушение условий эксплуатации средств защиты информации является инцидентом информационной безопасности.

4.16 Администратор информационной безопасности организует доступ сторонних лиц к ИСПДн и (или) ее элементам при проведении работ по созданию, модернизации, эксплуатации СЗПДн, при сопровождении ИСПДн, обслуживании технических средств, способом, исключающим возможность несанкционированного доступа к ПДн или их носителям, в том числе, возможность хищения носителя ПДн. В случае невозможности исключения доступа к ПДн администратор информационной безопасности обязан под роспись уведомить сторонних лиц, получающих доступ к ИСПДн и (или) ее элементам о необходимости обеспечивать конфиденциальность (целостность, доступность) ПДн и ответственности за правонарушения в сфере информационной безопасности в соответствии с действующим законодательством.

4.17 Работы по созданию, модернизации, эксплуатации СЗПДн, обслуживанию технических средств проводятся сторонними лицами в присутствии администратора информационной безопасности. Работы по обслуживанию ИСПДн могут проводиться в присутствии лица, ответственного за эксплуатацию ИСПДн (по решению администратора информационной безопасности).

4.18 Администратор информационной безопасности контролирует размещение всех технических средств, участвующих в обработке ПДн, а также входящих в состав вычислительной сети <НАЗВАНИЕ ОРГАНИЗАЦИИ> (в случае, если технические средства ИСПДн так же входят в состав вычислительной сети), в том числе, сетевого оборудования, в пределах защищаемых помещений (защищаемых зданий, частей здания), исключение возможности несанкционированного доступа к техническим средствам, расположенным вне контролируемой зоны.

4.19 При выводе из эксплуатации (либо передаче сторонним организациям в целях ремонта) отдельных элементов ИСПДн администратор информационной без-

опасности обязан обеспечить удаление из запоминающих устройств ПДн и технологической (служебной, конфигурационной, управляющей и т. д.) информации способом, предусмотренным технологией записи в запоминающее устройство.

На администратора информационной безопасности возлагаются обязанности по контролю соответствия технического паспорта ИСПДн фактическому составу (комплектности) средств вычислительной техники информационной системы и ведению учета изменений программно-аппаратной конфигурации, периодическому контролю целостности печатей (пломб, наклеек) на элементах защищенных рабочих мест (при наличии таковых). В этих целях администратор информационной безопасности ведет Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания средств вычислительной техники, выполнения профилактических работ, установки и модификации аппаратных и программных средств автоматизированных систем (ИСПДн). Кроме того, администратор информационной безопасности должен обеспечить фиксацию всех изменений технического характера в соответствующем техническом паспорте ИСПДн.

4.20 Если пользователь сообщает о невозможности входа в систему под своей учетной записью, администратор информационной безопасности должен:

– убедиться в том, что сотрудник правильно вводит имя пользователя;

– убедиться в том, что учетная запись не заблокирована;

– проанализировать содержимое журналов безопасности с целью выявления успешных и неуспешных попыток входа в систему с использованием данной учетной записи и узлов сети, с которых осуществлялся вход;

– сопоставить данные, полученные в результате анализа журналов безопасности, с информацией о режиме работы данного пользователя и его личной рабочей станции;

– установить причины нештатной ситуации и определить, имел ли место инцидент информационной безопасности;

– в случае если событие не отнесено к категории инцидентов информационной безопасности, устранить причины нештатной ситуации и обеспечить возможность входа пользователя в систему;

– в случае инцидента информационной безопасности осуществить процедуру реагирования на инцидент информационной безопасности в порядке, описанном в пункте 4.21 настоящей Инструкции.

При возникновении подозрения о компрометации пароля администратор информационной безопасности должен:

– обеспечить незамедлительную смену скомпрометированного пароля (или убедиться, что смена пароля уже произведена пользователем);

– установить время и дату предполагаемой компрометации пароля;

– проанализировать содержимое журналов безопасности начиная со дня, предшествующего предполагаемой дате компрометации, с целью обнаружения фактов входа в систему с использованием учетной записи пользователя, чей пароль был скомпрометирован, и узлов сети, с которых осуществлялся вход;

– сопоставить данные, полученные в результате анализа журналов безопасности, с информацией о режиме работы пользователя, использующего данную учетную запись, и его личной рабочей станции;

– установить, имел ли место инцидент информационной безопасности;

– в случае инцидента информационной безопасности осуществить процедуру реагирования на инцидент информационной безопасности в порядке, описанном в пункте 4.21 настоящей Инструкции.

4.21 При поступлении сообщения о возникновении нештатной ситуации (события, выходящего за рамки штатного функционирования <НАЗВАНИЕ ОРГАНИЗАЦИИ>) администратор информационной безопасности совместно с системным администратором осуществляет оперативный сбор информации, связанной с событием, и оценку этой информации с целью определения, относится ли событие к категории инцидентов информационной безопасности. К инцидентам информационной безопасности должны быть отнесены следующие события:

– уничтожение или блокирование данных, технических средств, инфраструктуры и элементов ИСПДн вследствие стихийного бедствия, пожара, затопления или техногенных факторов (сбои, отказы программного обеспечения, технических средств, систем обеспечения функционирования ИСПДн);

– нежелательная сетевая активность (сканирование сети, попытки подбора пароля, взлома системы защиты или воздействия на технические (в том числе, программные) средства);

– уничтожение, кража носителей ПДн, раскрытие, модификация или блокирование ПДн вследствие несанкционированного проникновения в контролируемую зону;

– утрата отчуждаемого носителя информации;

– уничтожение, модификация, блокирование, раскрытие информации или нарушение работоспособности ИСПДн вследствие успешно проведенной атаки или воздействия вредоносного программного обеспечения;

– уничтожение, модификация, блокирование, раскрытие информации или нарушение работоспособности ИСПДн, совершенные пользователем ИСПДн (или от его имени) с использованием назначенных ему прав;

– нарушение установленных в <НАЗВАНИЕ ОРГАНИЗАЦИИ> требований по безопасности.

При отнесении события к категории инцидентов информационной безопасности, администратор информационной безопасности совместно с системным администратором должен оценить уровень потенциального риска (путем определения возможности и характера ущерба, оценки темпа развития инцидента информационной безопасности):

– уровень 1 – инцидент информационной безопасности является локальным и может быть разрешен силами <НАЗВАНИЕ ОРГАНИЗАЦИИ>;

– уровень 2 – инцидент информационной безопасности может привести к существенному ущербу и может быть разрешен силами <НАЗВАНИЕ ОРГАНИЗАЦИИ> лишь частично;

– уровень 3 – последствия инцидента информационной безопасности являются критическими, и он не может быть разрешен силами <НАЗВАНИЕ ОРГАНИЗАЦИИ>.

В случае отнесения инцидента информационной безопасности к уровню 2 или уровню 3 незамедлительно уведомляется лицо, ответственное за организацию обработки ПДн, и <НАЗВАНИЕ ОРГАНИЗАЦИИ>.

Администратор информационной безопасности совместно с системным администратором (с привлечением при необходимости иных сотрудников и специалистов) осуществляют локализацию инцидента информационной безопасности. При локализации инцидента информационной безопасности указанные сотрудники с учетом оценки реальной ситуации и существующих возможностей под свою ответственность осуществляют выбор стратегии и способа реагирования на инцидент информационной безопасности. В рамках локализации инцидента информационной безопасности могут быть предприняты реактивные действия (отключение технических средств от внешних сетей или их изоляция; изменение настроек межсетевого экрана, маршрутизаторов, других технических средств; принятие иных экстренных мер) или проактивные действия (наблюдение, предупреждение дальнейшего развития инцидента информационной безопасности)). Допустимость реактивных действий определяется с учетом характера инцидента информационной безопасности и уровня потенциального риска в случае непринятия реактивных мер.

После локализации инцидента информационной безопасности администратором информационной безопасности составляется письменный отчет об инциденте информационной безопасности, его копия направляется лицу, ответственному за организацию обработки ПДн, и главному врачу <НАЗВАНИЕ ОРГАНИЗАЦИИ>. На администратора информационной безопасности возлагается ответственность за достоверность сведений, указанных в отчете об инциденте информационной безопасности. В отчете должны быть зафиксированы:

– дата и время, когда произошел инцидент информационной безопасности;

– перечень лиц (должность, фамилия, имя, отчество), бывших свидетелями события или сообщивших о нем;

– описание инцидента информационной безопасности;

– перечень свидетельств события и место их хранения (при наличии свидетельств);

– последовательность проведенных мероприятий и действий по локализации инцидента информационной безопасности, описание использованных при этом средств;

– описание ущерба и иных последствий инцидента информационной безопасности, в том числе вероятных последствий;

– выводы о возможных причинах инцидента информационной безопасности.

Данный документ хранится у администратора информационной безопасности.

Администратор информационной безопасности отвечает за обеспечение сохранности информации, относящейся к инциденту информационной безопасности. Указанная информация в дальнейшем может использоваться при проведении ком-

пьютерно-технической экспертизы, а также в качестве доказательной базы при судебном разбирательстве.

4.22 Администратору информационной безопасности запрещается:

– без согласования со специализированной организацией, осуществляющей сопровождение СЗПДн, изменять состав используемых на рабочих местах и серверах ИСПДн программных средств (в том числе, деинсталлировать установленные средства защиты информации; удалять или менять версию антивирусной программы; устанавливать программы, не участвующие в технологическом процессе обработки информации);

– изменять настройки средств защиты информации без согласования со специализированной организацией, осуществляющей сопровождение СЗПДн;

– использовать любые USB-устройства, не участвующие в технологическом процессе обработки информации и не зарегистрированные в соответствующем журнале;

– передавать сторонним организациям в целях ремонта носители информации, которые могут содержать ПДн (жесткие диски, USB-носители и т. п.);

– использовать предоставленные полномочия в целях, отличных от целей, предусмотренных служебными обязанностями;

– производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы автоматизированной системы (ИСПДн), блокировке, потере информации, без предупреждения пользователей[1].

5 Права администратора информационной безопасности

5.1 Администратор информационной безопасности имеет право:

– осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим докладом лицу, ответственному за организацию обработки ПДн, и главному врачу <НАЗВАНИЕ ОРГАНИЗАЦИИ>;

– вносить свои предложения по совершенствованию мер защиты обрабатываемых ПДн.

Разработал:
Лицо, ответственное за организацию
обработки персональных данных _____ *Ф.И.О.*

_____

Ознакомлен:
наименование должности _____ *Ф.И.О.*
Дата ознакомления: _____

[1] Действие данного пункта не распространяется на критичные (нештатные) ситуации, при которых необходимо прекращение дальнейшей обработки информации с целью сохранения заданных характеристик безопасности обрабатываемых данных.