Государственное бюджетное учреждение
здравоохранения Астраханской области
«ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №2
имени братьев Губиных»

П Р И К А З

«___» _____ 2019 г. №_____

О проведении мероприятий по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных

Во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в Государственном бюджетном учреждении здравоохранения Астраханской области «Городская клиническая больница №2 имени братьев Губиных» (далее по тексту - Учреждение») (Приложение № 1).
2. Для оценки возможного вреда субъектам, чьи персональные данные обрабатываются в информационных системах Учреждения назначить комиссию в составе:

Председатель — Заведующая организационно методическим кабинетом Зенкович М.В.

Члены комиссии: Техник по защите информации Черемской А.Н.
Главный бухгалтер Калюжная С.И.
Начальник отдела кадров Кочекаева Х.Ж
Юрист Е.В. Спиридонова

3. По результатам работ предоставить для утверждения Акт оценки возможного вреда субъектам, чьи персональные данные обрабатываются в информационных системах Учреждения согласно приложения №1 к настоящему приказу.
4. Контроль за исполнением настоящего приказа возложить Зенкович М.В.

Главный врач Р.Б. Якушев

Приложение №1
к приказу
от _____ № _____

ПРАВИЛА

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в государственном бюджетном учреждении здравоохранения Астраханской области «Городская клиническая больница №2 имени братьев Губиных»

1. Общие положения

1.1. Настоящие Правила в государственном бюджетном учреждении здравоохранения Астраханской области «Городская клиническая больница №2 имени братьев Губиных» оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения федерального законодательства по защите персональных данных, в частности Федерального закона № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных № 152-ФЗ.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2. Термины и определения

2.1. В настоящих Правилах используются основные понятия:

2.1.1. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.1.2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

2.1.3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.1.4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

2.1.5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.1.6. Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

2.1.7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

2.1.8. Оценка возможного вреда - определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. Описание вреда субъектам персональных данных

3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.

3.2.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных.

3.2.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

3.2.4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации.

3.2.5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.

3.2.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

3.2.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.

3.2.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме

субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинён вред в форме:

3.3.1. Убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

3.3.2. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

4. Методика оценки возможного вреда субъектам персональных данных

4.1. Оценка возможного вреда должна производиться коллегиально. В комиссии должно быть не менее трех человек.

4.2. В оценке возможного вреда исходить из учёта последствий допущенного нарушения принципов обработки персональных данных. Вводится четыре уровня возможного вреда:

нулевой - вред субъекту ПДн не причиняется;

низкий - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

средний - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

высокий - во всех остальных случаях.

4.3. Каждому уровню возможного вреда сопоставляется числовая оценка Y1, а именно:

0 - при нулевом уровне вреда;

0,05 - при низком уровне вреда;

0,1 - при среднем уровне вреда;

0,2 - при высоком уровне вреда.

4.4. Каждым членом комиссии на основании собственного субъективного мнения выставляется одна из возможных оценок возможного вреда субъекту для каждой актуальной угрозы безопасности его ПДн из-за несанкционированного, в том числе случайного, доступа к его ПДн при их обработке в информационных системах.

4.5. Все коэффициенты оценок суммируются по каждой актуальной угрозе.

4.6. По значению суммарной оценки Y2 определяется возможный вред следующим образом:

если $Y2 > 0,9$, то вред субъектам ПДн признается высоким;

если $0,5 < Y2 \leq 0,9$, то вред субъектам ПДн признается средним;

если $0,2 < Y2 \leq 0,5$, то вред субъектам ПДн признается низким;
если $0 < Y2 \leq 0,5$, то вред субъектам ПДн признается нулевым.

5. Требования к мерам защиты

5.1. С использованием данных об уровне защищенности ИСПДн Учреждения и категориях персональных данных, обрабатываемых в них, на основе «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» формулируются и применяются конкретные организационные и технические меры защиты, которые могут быть использованы при эксплуатации ИСПДн.

Акт
оценки возможного вреда субъектам, чьи персональные данные обрабатываются в информационных системах государственного бюджетного учреждения здравоохранения Астраханской области «Городская клиническая больница №2 имени братьев Губиных»

Комиссия в составе:

Председатель	Заведующая организационно методическим кабинетом Зенкович М.В.
Члены комиссии:	Техник по защите информации Черемской А.Н.
	Главный бухгалтер Калюжная С.И.
	Начальник отдела кадров Кочекаева Х.Ж
	Юрист Е.В. Спиридонова

с целью
самостоятельной экспертной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения в государственном бюджетном учреждении здравоохранения Астраханской области «Городская клиническая больница №2 имени братьев Губиных» (далее по тексту - Учреждение» обязанностей, предусмотренных Федеральным законом № 152-ФЗ от 27 июля 2006 г. «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

рассмотрев
результаты по сбору и анализу исходных данных на информационные системы персональных данных,

во исполнение требований
пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», о том, что оператор персональных данных самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о ПДн, и, в частности, к таким мерам относится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Обществом законодательства в сфере персональных данных,

с учетом разработанных Учреждением правил оценки вреда, который может быть причинен субъектам персональных данных, ОПРЕДЕЛИЛА:

ТИПЫ актуальных угроз безопасности ПДн	**ОЦЕНКИ возможного вреда субъекту ПДн, определенные членами комиссии**					**Определение возможного вреда (Y2)**
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5	
Кража ПЭВМ	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2 = 1,0 вред субъектам ПДн высокий
Кража носителей информации	Высокий (0,2)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2 = 0,5 вред субъектам ПДн низкий
Кража ключей и паролей доступа внутренними и внешними нарушителями	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2 = 1,0 вред субъектам ПДн высокий
Кража, модификация, уничтожение информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Y2 = 0,45 вред субъектам ПДн низкий
Вывод из строя узлов ПЭВМ, каналов связи	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,2 вред субъектам ПДн нулевой
Несанкционированный доступ	Нулевой (0)	Средний	Средний	Средний	Низкий	Y2 = 0,35

к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ		(0,1)	(0,1)	(0,1)	(0,05)	вред субъектам ПДн низкий
Несанкционированное отключение средств защиты	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2 = 0,6 вред субъектам ПДн средний
Действия вредоносных программ (вирусов)	Средний (0,1)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2 = 0,8 вред субъектам ПДн средний
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкий (0,05)	Средний (0,1)	Высокий (0,2)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,45 вред субъектам ПДн низкий
Установка ПО, не связанного с исполнением служебных обязанностей	Нулевой (0)	Средний (0,1)	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,2 вред субъектам ПДн нулевой
Внедрение аппаратных закладок	Нулевой (0)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2 = 0,3 вред субъектам ПДн низкий
Утрата паролей доступа к	Низкий	Низкий	Высокий	Средний	Средний	Y2 = 0,5

ИСПДн	(0,05)	(0,05)	(0,2)	(0,1)	(0,1)	вред субъектам ПДн низкий
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,3 вред субъектам ПДн низкий
Непреднамеренное отключение средств защиты	Высокий (0,2)	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Y2 = 0,65 вред субъектам ПДн средний
Выход из строя аппаратно-программных средств	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2 = 0,3 вред субъектам ПДн низкий
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2 = 0,9 вред субъектам ПДн средний
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Y2 = 0,8 вред субъектам ПДн средний
Несанкционированный доступ	Высокий	Средний	Средний	Низкий	Низкий	Y2 = 0,5

через ЛВС организации	(0,2)	(0,1)	(0,1)	(0,05)	(0,05)	вред субъектам ПДн низкий
Перехват информации за пределами контролируемой зоны	Высокий (0,2)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Y2 = 0,55 вред субъектам ПДн средний
Удаленный запуск приложений	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Y2 = 0,5 вред субъектам ПДн низкий
Сканирование сети	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Нулевой (0)	Высокий (0,2)	Y2 = 0,4 вред субъектам ПДн низкий

Вывод:

На основании оценок, выставленных членами комиссии, данных об уровне защищенности ИСПДн Учреждения и категориях персональных данных, обрабатываемых в них, с учетом требований, предусмотренных статьями 18.1 и 19 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» в Учреждении приняты следующие меры:

1. Назначен ответственный за обработку персональных данных и администратор информационных систем персональных данных;
2. Осуществляется внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных;
3. Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;
4. Разработаны правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
5. Обеспечивается учет машинных носителей персональных данных;
6. Обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
7. Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8. Определён перечень сотрудников, осуществляющих обработку персональных данных, сведения на бумажных носителях хранятся в сейфах или выделенных помещениях, определены места хранения персональных данных;
9. Ведётся учёт всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);
10. Утверждены инструкции, регламентирующие работу с персональными данными и информационными системами персональных данных:
    1) Инструкция Администратора ИСПДн;
    2) Инструкция Ответственного за обработку ПДн;
    3) Инструкция По антивирусной защите;
    4) Инструкция По работе с документами;
    5) Инструкция По учету машинных носителей;
    6) Инструкция Пользователя ИСПДн;
    7) Инструкция О порядке резервирования и восстановления;
    8) Положение Об обработке персональных данных;
    9) Разрешительная система доступа;
    10) Регламент реагирования на запрос субъекта;
    11) Перечень должностных лиц, имеющих доступ к персональным данным;
    12) Порядок доступа в помещения, где ведётся обработка персональных данных;
    13) Правила работы с обезличенными данными;

14) Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

11. Исключена возможность неконтролируемого пребывания посторонних лиц в помещениях где ведется обработка персональных данных;

12. На компьютерах установлено антивирусное программное обеспечение;

13. Пользователи работают под ограниченными учетными записями;

14. Вход в информационную систему осуществляется по буквенно-цифровому паролю;

15. Используются средства резервного копирования.

Председатель комиссии:

_____

должность подпись Ф.И.О.

Члены комиссии:

_____

должность подпись Ф.И.О.

_____

должность подпись Ф.И.О.

_____

должность подпись Ф.И.О.

_____

должность подпись Ф.И.О.

«___» _____ 20__ года