УТВЕРЖДАЮ

Директор
ОБУК «Госдирекция»

_____ А.А. Найденов

«01» 06 2021 г.

МП

ПОЛОЖЕНИЕ

об организации режима безопасности помещений, где осуществляется работа с персональными данными

Липецк 2021

Оглавление

1. Термины, определения и сокращения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Автоматизированная система (АС) - Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О 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 (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) - материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных - 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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу(Федеральный закон от 27.07.2006 № 152-ФЗ «О 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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Физическая защита информации - защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

2. Общие положения

2.1. Настоящее Положение разработано на основании следующих правовых и нормативных документов:

2.1.1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2.1.2. Федеральный закон от 27 июня 2006 № 152-ФЗ «О персональных данных»;

2.1.3. Указ Президента РФ от 06 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;

2.1.4. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

2.1.5. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2.1.6. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

2.1.7. Положение о сертификации средств защиты информации, утвержденное постановлением Правительства РФ от 26 июня 1995 года № 608;

2.1.8. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

2.1.9. Методический документ «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г.

2.1.10. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 30 июля 2012 г. № 240/24/3095 «Об утверждении требований к средствам антивирусной защиты»;

2.1.11. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 20 ноября 2012 г. № 240/24/4669 «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных»;

2.1.12. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 15 июля 2013 г. № 240/22/2637 «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и приказа ФСТЭК России от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"».

2.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность сотрудников обрабатывающих персональные данные, руководителей

структурных подразделений и лиц, на которых возложены обязанности ответственного за организацию обработки персональных данных (далее – ответственный) за обеспечение безопасности служебных кабинетов, где располагаются ПЭВМ входящие в систему обработки персональных данных.

2.3. Сотрудник, исполняющий обязанности ответственного назначается из числа сотрудников, рабочее место которого находится в конкретном кабинете. Ответственный назначается директором ОБУК «Госдирекция», и является лицом, выполняющим функции по обеспечению безопасности (охраны) кабинета. В пределах своей зоны ответственности функции ответственного могут быть распределены между несколькими сотрудниками.

2.4. В своей деятельности ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных (указанных в п. 2.1) и обеспечивает их выполнение.

2.5. Настоящая Инструкция является дополнением к действующим регламентирующим документам ОБУК «Госдирекция» по вопросам пропускного режима и защиты информации и не исключает обязательного выполнения их требований.

3. Методы и средства охраны помещений в организации

3.1. Первичный (основной) метод – система контроля и управления доступом в здание организации, включает в себя:

3.1.1. наличие при входе в здание пункта контрольного пропуска;

3.1.2. определение внешнего контролируемого периметра.

3.2. Вторичный (дополнительный) метод – система контроля перемещения лиц в здании и управления доступом в помещения, включает в себя:

3.2.1. наличие помещений с активным сетевым оборудованием с определенными правами доступа;

3.2.2. наличие пожарной сигнализаций в помещениях организации;

3.2.3. использование замков в помещениях;

3.2.4. использование сейфов, шкафов, а также хранение информации с ПДн на внутренних и внешних носителях.

4. Методы контроля доступа в помещения

4.1. Ограничение доступа посторонних лиц в помещения, предназначенные для осуществления профессиональной деятельности, связанной с эксплуатацией информационных систем, предусматривает следующие мероприятия:

4.1.1. Размещение помещений и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая работников других подразделений.

4.1.2. После окончания рабочего дня дверь рабочих помещений и помещений, в которых эксплуатируется информационные системы, закрывается на ключ. Все помещения имеют разные замки. Дубликаты ключей хранятся в запираемом шкафу. В случае выхода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ.

4.1.3. Доступ посторонних лиц в помещения после окончания рабочего дня, установленного в подразделении, ограничен. Уборка помещения производится в присутствии одного из сотрудников этого помещения.

4.1.4. Доступ работников в помещения подразделения по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.

4.1.5. Строгое ограничение доступа посторонних лиц к сетевому оборудованию.

4.1.6. В случае утраты ключей, об этом немедленно докладывается руководителю, и принимаются меры к немедленной замене замков.

5. Методы защиты носителей информации в помещении

5.1. Защита мест хранения носителей конфиденциальной информации (USB flash-накопитель, CD, внешних ЖМД) от беспрепятственного доступа и наблюдения, защита персональных данных от неправомерного использования, предусматривает следующие мероприятия:

5.1.1. Приказом директора ОБУК «Госдирекция» определяются места хранения носителей.

5.1.2. Все носители, содержащие конфиденциальную информацию (в том числе и персональные данные), хранятся в шкафах или сейфах, запираемых на ключ, который хранится у ответственных работников. В конце каждого рабочего дня носители убираются в указанные шкафы или сейфы.

5.1.3. Регулярное проведение инвентаризации мест хранения носителей, содержащих конфиденциальную информацию (в том числе и персональные данные). Факты обнаружения недостачи, порчи, утери носителей доводятся до сведения руководителя. К виновным лицам применяются меры дисциплинарной ответственности.

6. Структура должностных прав и обязанностей при организации охраны помещений.

6.1. Директор ОБУК «Госдирекция»

6.1.1. отвечает:

- за организацию работы;
- за охрану помещений.

6.1.2. имеет право:

- утверждать регламентирующие документы;
- утверждать лиц, ответственных за определенные сферы деятельности Организации;
- назначать комиссию для проведения внутреннего расследования;
- принимать решения о наказании виновных лиц;
- организовать работу старших кабинетов;
- проводить мероприятия постоянного и выборочного контроля.

6.2. Администратор безопасности

6.2.1. отвечает:

- за организацию контрольных мероприятий;
- за представление директору ОБУК «Госдирекция» информации о состоянии работы по охране помещений;
- за проведение работ по инвентаризации носителей информации, хранящихся в помещениях;
- за контроль хранения носителей информации в установленных местах в помещении.

6.2.2. имеет право:

- проводить плановую и внеплановую проверку организации работ;
- вносить предложения директору ОБУК «Госдирекция» о совершенствовании работ.

6.3. Ответственный за организацию обработки персональных данных

6.3.1. отвечает:

- за обеспечение непосредственной охраны помещения;
- за контроль обеспечения ограничения доступа в помещение.
- за обеспечение режима «закрытые двери» при отсутствии сотрудников в помещении.

- за организацию контроля наличия ключей у сотрудников.
- за сдачу под охрану (при необходимости) помещения дежурному сотруднику охраны здания.
- за извещение начальника Организации и Администратора безопасности о фактах нарушения охраны помещения и утрате ключей.

6.3.2. имеет право:

- вносить предложения начальнику Организации и Администратору безопасности о совершенствовании работ.

6.4. Оператор ПЭВМ

6.4.1. обязан:

- хранить носители информации в строго отведенном месте;
- обеспечивать исключающее визуальный просмотр информации расположение монитора ПЭВМ при посещении кабинета посторонними лицами;
- обеспечивать минимальное количество (необходимое для работы в данный момент) бумажных носителей на рабочем столе;
- не передавать ключ от кабинета посторонним лицам;
- закрывать дверь на ключ при выходе из помещения при отсутствии сотрудников;
- немедленно докладывать старшему кабинета в случае утраты ключа.

6.4.2. имеет право:

- использовать носители информации в пределах помещения в соответствии с должностными обязанностями;
- вносить предложения начальнику Организации и Администратору безопасности о совершенствовании работ.

Председатель ПДК А.А. Найденов

«01» октября 2021 г.

Приложение 1

Лист ознакомления

№ п/п	Ф.И.О.	Роспись	Дата
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			
38.			
39.			
40.			
41.			
42.			
43.			