Приложение № 2

САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «УЧИЛИЩЕ ОЛИМПИЙСКОГО РЕЗЕРВА № 1»

УТВЕРЖДЕНО
приказом СПб ГБПОУ «УОР № 1»
от 12.12.2023 № 508

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности информации на объектах информатизации Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Училище олимпийского резерва № 1»

Санкт-Петербург
2023

СОДЕРЖАНИЕ

1. Термины и определения 6
2. Нормативно-методическое обеспечение 8
3. Общие положения 9
4. Администратор информационной безопасности 10
4.1. Функции администратора информационной безопасности 10
4.2. Обязанности администратора информационной безопасности 11
4.3. Ответственность администратора информационной безопасности 11
4.4. Права администратора информационной безопасности 11
5. Инструкция пользователей ИСПДн 12
5.1. Общие положения 12
5.2. Должностные обязанности 12
5.3. Правила работы в сетях общего доступа и (или) международного обмена 14
5.4. Порядок реагирования на аварийную ситуацию 14
5.5. Права и ответственность пользователей ИСПДн 14
6. Ознакомление лица, допущенного к обработке персональных данных, с нормами текущего законодательства 15
7. Организация режима обеспечения безопасности помещений, в которых осуществляется обработка защищаемой информации 16
7.1. Общие сведения 16
7.2. Требования к помещениям, предназначенным для размещения архивов 17
7.3. Обеспечение безопасности серверного помещения 17
7.4. Порядок доступа работников и третьих лиц к обработке ПДн и в помещения, в которых осуществляется обработка 18
8. Внутренний и внешний контроль соответствия обработки ПДн текущему законодательству и принятым локальным НПА 19
8.1. Внешний контроль над соблюдением требований по обработке и обеспечению безопасности защищаемой информации 19
8.2. Внутренний контроль соответствия обработки защищаемой информации требованиям к защите информации 19
8.2.1. Порядок внутреннего контроля соответствия обработки защищаемой информации требованиям к защите информации 19
8.2.2. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» 21
9. Порядок проведения служебной проверки по фактам нарушения требований по обеспечению безопасности защищаемой информации 23
9.1. Классификация нарушений требований по обеспечению безопасности защищаемой информации 23

9.2. Перечень нарушений требований по обеспечению безопасности защищаемой информации 23
9.3. Назначение и проведение служебной проверки 25
9.4. Оформление результатов работы комиссии 25
10. Порядок приостановления обработки защищаемой информации 27
11. Обезличивание ПДн 28
11.1. Условия обезличивания ПДн 28
11.2. Методы обезличивания ПДн 28
11.3. Процедура обезличивания 28
11.4. Организация обработки ПДн и обезличенных данных 28
11.5. Рекомендации по выбору методов обезличивания в соответствии с классом задач обработки 29
12. Уничтожение защищаемой информации, в том числе машинных носителей 31
12.1. Условия уничтожения защищаемой информации 31
12.2. Порядок уничтожения защищаемой информации 31
12.3. Способы уничтожения защищаемой информации 31
12.4. Подтверждение уничтожения персональных данных 32
13. Порядок управления доступом субъектов доступа к объектам доступа ОИ 34
14. Организация парольной защиты на ОИ 34
14.1. Общие положения 34
14.2. Порядок организации парольной защиты 34
14.3. Порядок применения парольной защиты 35
15. Организация антивирусной защиты на ОИ 36
15.1. Общие положения 36
15.2. Порядок организации антивирусной защиты 36
16. Организация учета и хранения машинных носителей информации 37
16.1. Порядок учета машинных носителей информации 37
16.2. Порядок хранения машинных носителей информации 38
16.3. Порядок эксплуатации машинных носителей информации 38
17. Организация резервирования и восстановления информации на ОИ 38
17.1. Общие положения 38
17.2. Информация, подлежащая резервному копированию 38
17.3. Порядок резервирования и хранения резервных копий 39
17.4. Порядок восстановления работоспособности ОИ 39
18. Порядок работы с электронными журналами протоколирования и анализа (аудита) значимых событий 39
19. Порядок обращения со средствами защиты информации 40
19.1. Учет средств защиты информации 40
19.2. Уничтожение средств защиты информации 40
19.3. Ответственность за нарушение требований эксплуатации средств защиты 40

20. Порядок обеспечения информационной безопасности ИС при модернизации (обновлении) аппаратных и программных компонентов 41
21. Контроль и надзор за эксплуатацией аттестованных ОИ 41
22. Порядок действий работников в нештатных ситуациях 42
23. Ответственность за нарушение требований законодательства 46
Приложение № 1 47
Приложение № 2 49
Приложение № 3 50
Приложение № 4 51
Приложение № 5 53
Приложение № 6 55
Приложение № 7 57
Приложение № 8 59

Список сокращений и обозначений

АС	Автоматизированная система
БД	База данных
НСД	Несанкционированный доступ
ОИ	Объект информатизации
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
ТС	Техническое средство
ИС	Информационная система
ИСПДн	Информационная система персональных данных
НПА	Нормативно-правовые акты
СВТ	Средство вычислительной техники
ИБ	Информационная безопасность

1. Термины и определения

Автоматизированная система (далее — АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа (далее — НСД) к информации и (или) воздействия на информацию или ресурсы АС.

Доступ к информации — возможность получения информации и ее использования.

Защита информации от НСД — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации правил или правил разграничения доступа к защищаемой информации. Заинтересованными субъектами, осуществляющими НСД к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защищаемый объект информатизации (далее — ОИ) — ОИ, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

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

Информационная система (далее — ИС) — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

ИС персональных данных (далее — ИСПДн) — совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Информационная технология — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Компьютерный вирус — вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

Контролируемая зона — пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.

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

Норма эффективности защиты информации – значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

Обезличивание ПДн — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Объект доступа (в автоматизированной ИС) **— е**диница ресурса автоматизированной ИС, доступ к которой регламентируется правилами разграничения доступа.

ОИ — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

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

ПДн — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Программное воздействие — несанкционированное воздействие на ресурсы автоматизированной ИС, осуществляемое с использованием вредоносных программ.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Субъект доступа (в автоматизированной информационной системе) — лицо или единица ресурса автоматизированной ИС, действия которой по доступу к ресурсам автоматизированной ИС регламентируются правилами разграничения доступа.

Требование по защите информации – установленное правило или норма, которая должна быть выполнена при организации осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Уязвимость ИС — свойство ИС, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Целостность (информации (ресурсов автоматизированной информационной системы) — состояние информации (ресурсов автоматизированной ИС), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Нормативно-методическое обеспечение

Настоящее Положение по организации и проведению работ по обеспечению безопасности информации на объектах информатизации Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Училище олимпийского резерва № 1» (далее — Положение, Учреждение) разработано на основании:

[1] — Федерального закона Российской Федерации (далее — РФ) от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] — Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

[3] — Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[4] — Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

[5] — 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»;

[6] — Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

[7] — Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 27 октября 2022 г. № 178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;

[8] — «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

[9] — ГОСТ Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации»;

[10] — ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»;

[11] — ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

3. Общие положения

Настоящее Положение определяет порядок организации и проведения работ по обеспечению безопасности персональных данных и информации, не составляющей государственную тайну, содержащейся в информационных системах (далее – защищаемая информация), обрабатываемых на объектах информатизации (далее — ОИ) Учреждения.

Положение разработано с целью:

— организации и координации работ по обеспечению безопасности ИСПДн, операторами которых является Учреждение, защищаемой информации на ОИ, взаимодействующих с другими информационными системами;

— регламентации порядка проведения работ по обеспечению безопасности защищаемой информации, обрабатываемой на ОИ;

— контроля состояния безопасности защищаемой информации, обрабатываемой на ОИ;

— определение такого порядка обработки ПДн, при котором обеспечиваются законные права и интересы субъектов ПДн.

Положение обязательно для исполнения всеми лицами, участвующими в обработке защищаемой информации.

4. Администратор информационной безопасности

4.1. Функции администратора информационной безопасности

Администратор информационной безопасности осуществляет следующие мероприятия, направленные на обеспечение безопасности защищаемой информации, обрабатываемой на ОИ:

4.1.1. Настройка и сопровождение системы защиты ОИ:

— реализует полномочия доступа для каждого пользователя ОИ на основе утвержденного руководителем Учреждения перечня лиц, имеющих доступ к защищаемой информации, обрабатываемой на ОИ;

— своевременно удаляет учетные записи пользователей на ОИ при увольнении или перемещении работника;

— своевременно блокирует и производит разблокировку учетных записей пользователей ОИ при их уходе на больничный или в отпуск и при выходе с больничного или из отпуска;

— периодически, но не реже одного раза в квартал, контролирует смену паролей пользователями для доступа на ОИ;

— регистрирует новых пользователей ОИ;

— периодически, но не реже одного раза в месяц, выполняет мероприятия по периодическому тестированию функционирования СЗИ в соответствии с документацией разработчика данных средств, регистрируя проведение данных мероприятий.

4.1.2. Настройка и сопровождение подсистемы регистрации и учета ОИ:

— проводит регулярный анализ системного журнала ОИ для выявления попыток НСД к защищаемым ресурсам с соответствующей регистрацией проверки;

— своевременно информирует руководство о несанкционированных действиях персонала и участвует в разбирательствах по фактам попыток НСД;

— проводит резервное копирование информационных массивов ОИ.

4.1.3. Сопровождение подсистемы обеспечения целостности ОИ:

— осуществляет учет возникновения нештатных ситуаций;

— осуществляет восстановление информационной системы при возникновении сбоев.

4.1.4. Контроль функционирования подсистемы антивирусной защиты ОИ:

— обеспечивает поддержание установленного порядка и соблюдение правил антивирусной защиты;

— периодически, но не реже одного раза в месяц, проводит антивирусные проверки всех жестких дисков, SSD ОИ;

— регистрирует результаты антивирусных проверок.

4.1.5. Контроль использования машинных носителей информации и ведение их учета.

4.1.6. Сопровождение подсистемы межсетевого экранирования ОИ.

4.1.7. Сопровождение подсистемы обнаружения вторжений ОИ.

4.1.8. Организация обновлений ПО и средств защиты, выполнение профилактических работ, установки и модификации программных средств на ОИ.

4.1.9. Проведение модернизации аппаратных компонентов.

4.1.10. Проведение инструктажа работников, имеющих право доступа к защищаемой информации.

4.1.11. Осуществление контроля за соблюдением пользователями ИС требований к защите информации.

4.1.12. Осуществление контроля за обеспечением уровня защищенности ПДн на ОИ, а также контроля за соблюдением пользователями ОИ требований к защите ПДн.

4.1.13. Участие в анализе ситуаций, касающихся функционирования СЗИ и проверки фактов НСД.

4.1.14. Оказание методической помощи по вопросам обеспечения безопасности защищаемой информации.

4.1.15. Разработка предложений и участие в проводимых работах по совершенствованию системы защиты информации, обрабатываемой на ОИ.

4.1.16. Проведение внутреннего контроля соответствия обработки ПДн к защите ПДн.

4.1.17. Администратор информационной безопасности может делегировать полномочия другому лицу.

4.2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

— обеспечивать функционирование и поддерживать работоспособность средств защиты ОИ, в пределах, возложенных на него функций;

— в случае отказа работоспособности ТС и ПО, средств вычислительной техники, в том числе средств защиты ОИ, принимать меры по их своевременному восстановлению и выявлению причин, которые вызвали отказ работоспособности;

— информировать руководство о фактах нарушения установленного порядка работ, попытках и фактах НСД к защищаемой информации, обрабатываемой на ОИ.

4.3. Ответственность администратора информационной безопасности

Администратор информационной безопасности несет ответственность за:

— неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящим Положением в пределах, определенных законодательством РФ;

— совершенные в процессе осуществления своей деятельности правонарушения — в пределах, определенных административным, уголовным и гражданским законодательством РФ;

— невыполнение или ненадлежащее выполнение указаний руководства;

— сохранность защищаемой информации;

— соблюдение требований нормативных правовых актов и локальных актов Учреждения, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности информации, обрабатываемой на ОИ;

— сохранность и работоспособное состояние ТС, ПО, средств защиты, входящих в состав ОИ;

— выполнение обязанностей, предусмотренных настоящим Положением;

— нарушения допущенные лицом, которому администратор информационной безопасности делегировал свои полномочия.

4.4. Права администратора информационной безопасности

Администратор информационной безопасности вправе:

— контролировать работу пользователей ОИ;

— требовать прекращения обработки информации, как в целом, так и отдельных пользователей ОИ, в случае выявления нарушений требований по обработке и обеспечению безопасности защищаемой информации, обрабатываемой на ОИ Учреждения.

5. Инструкция пользователей ИСПДн

5.1. Общие положения

Пользователем является каждый работник Учреждения, участвующий в рамках своих должностных обязанностей в процессах обработки персональных данных (далее — ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

Пользователь ИСПДн (далее — Пользователь) осуществляет обработку ПДн в ИСПДн.

Пользователь несет персональную ответственность за свои действия.

Пользователь в своей работе руководствуется настоящей инструкцией, и нормативными документами Учреждения в части касающейся обеспечения защиты информации.

Методическое руководство работой пользователя осуществляется ответственным за организацию обработки персональных данных и работниками структурного подразделения, обеспечивающего работу механизмов защиты информации.

5.2. Должностные обязанности

Пользователь обязан:

5.2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций по защите информации и документов, регламентирующих порядок действий по защите информации.

5.2.2. Выполнять на рабочем месте только те процедуры, которые определены для него в должностной инструкции, а также в других нормативных актах Учреждения.

5.2.3. Знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

5.2.4. Соблюдать требования инструкции по организации парольной защиты.

5.2.5. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты) так, чтобы исключить возможность визуального просмотра монитора за пределами помещения.

5.2.6. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к ответственному за организацию защиты персональных данных в ИСПДн. Для получения консультации в части касающейся информационной безопасности возможно обратиться к работникам структурного подразделения, обеспечивающего работу механизмов защиты информации.

5.2.7. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к ответственному по этой части структурному подразделению.

5.2.8. При отсутствии визуального контроля за рабочей машиной доступ к ней должен быть немедленно заблокирован. Для этого необходимо нажать одновременно

комбинацию клавиш <Windows><L> (для ОС семейства Windows); для ОС семейства Linux необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><L> или <Windows><L>.

5.2.9. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

5.2.10. Соблюдать режим допуска в помещения, где осуществляется обработка ПДн.

5.2.11. Использовать только учтенные машинные носители информации.

5.2.12. Перед началом работы с машинным носителем информации осуществлять проверку носителя на предмет отсутствия компьютерных вирусов.

5.2.13. В случае получения работником электронно-цифровой подписи, необходимой для выполнения должностных обязанностей, самостоятельно, необходимо уведомить об этом ответственного пользователя криптосредств или орган криптографической защиты и расписаться в соответствующем журнале.

5.2.14. Перед тем, как покинуть помещение, где ведется обработка ПДн, необходимо запереть помещение на ключ.

5.2.15. Пользователям запрещается:

— разглашать защищаемую информацию третьим лицам;

— копировать защищаемую информацию на внешние неучтенные машинные носители информации;

— самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

— несанкционированно открывать общий доступ к папкам на своей рабочей машине;

— запрещено подключать к рабочей машине и информационной сети личные внешние носители (неучтенные) и мобильные устройства;

— отключать (блокировать) средства защиты информации;

— обрабатывать на рабочей машине постороннюю информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

— сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн (логины, пароли и т.д.);

— привлекать посторонних лиц для производства ремонта или настройки рабочих машин, без согласования с ответственным лицом.

— хранить на одном машинном носителе информации ПДн, цели обработки которых заведомо не совместимы;

— открывать общий доступ к папкам на своей рабочей машине, если в этом нет должностной необходимости;

— оставлять посторонних лиц без присмотра в помещениях, в которых осуществляется обработка ПДн;

— производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

— передавать защищаемую информацию по открытым каналам без использования необходимых средств защиты.

5.3. Правила работы в сетях общего доступа и (или) международного обмена

5.3.1. Работа в сетях общего доступа (Интернет и других) (далее — Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

5.3.2. При работе в Сети запрещается:

— осуществлять работу при отключенных средствах защиты (антивирус и других);

— передавать по Сети защищаемую информацию без использования средств шифрования;

— запрещается скачивать из Сети программное обеспечение и другие файлы;

— запрещается нецелевое использование подключения к Сети.

5.4. Порядок реагирования на аварийную ситуацию

5.4.1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже.

— отключение электроэнергии;

— сбой в работе вычислительной сети (коммутационного оборудования);

— ошибка персонала;

— нарушение конфиденциальности, целостности и доступности персональных данных;

— физический разрыв внешних каналов связи.

5.4.2. В случае реализации любой из угроз (выявлении предпосылок к ее реализации) Пользователь обязан:

— предпринять попытку сохранения обрабатываемой информации, содержащей ПДн;

— прекратить работу на рабочем месте;

— немедленно оповестить ответственное лицо за обеспечение безопасности ИСПДн (или администратору информационной безопасности) о возникновении аварийной ситуации.

5.5. Права и ответственность пользователей ИСПДн

5.5.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.5.2. Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. № 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

6. Ознакомление лица, допущенного к обработке персональных данных, с нормами текущего законодательства

Первичный инструктаж лица, допущенного к обработке ПДн на ОИ, проводится после утверждения руководителем документа о наделении лица правом доступа к обработке ПДн до непосредственного доступа этого лица к ОИ.

Лицо получает непосредственный доступ к защищаемой информации только после прохождения первичного инструктажа.

Лицо, допущенное к работе с защищаемой информацией, должно быть ознакомлено с нормативными правовыми актами РФ, в том числе города Санкт-Петербург, и с локальными актами Учреждения, регламентирующими работу с персональными данными, в том числе в которых содержатся требования к защите персональных данных.

Лицо, являющееся пользователем ОИ, должно иметь доступ только к тем информационным ресурсам ОИ, которые необходимы для выполнения им его должностных обязанностей.

Администратор информационной безопасности, проводящий инструктаж лица, обязан разъяснить ему, какие действия на ОИ лицо имеет право совершать, а какие действия ему запрещены.

Лицо, допущенное к работе с защищаемой информацией, обрабатываемой на ОИ, должно быть предупреждено:

— об обязанностях выполнения всех правил и требований, предусмотренных локальными актами Учреждения в области защиты информации;

— о проведении разбирательств по фактам совершения действий, связанных с доступом к защищаемой информации, обрабатываемой на ОИ, и повлекших за собой негативные последствия, в соответствии с установленным Порядком проведения разбирательств по фактам нарушения требований по обеспечению безопасности защищаемой информации.

Факт прохождения лицом первичного инструктажа регистрируется специалистом по защите информации в соответствующем журнале. В случае необходимости, нужно ознакомлять работников с изменениями в законодательстве в области обработки и защиты ПДн, в том числе в локальных актах Учреждения.

7. Организация режима обеспечения безопасности помещений, в которых осуществляется обработка защищаемой информации

7.1. Общие сведения

Помещения, в которых осуществляется обработка защищаемой информации, должны располагаться в пределах контролируемой зоны.

Доступ иных лиц в помещения Учреждения, где осуществляется обработка защищаемой информации, разрешается только в присутствии лиц, имеющих право доступа в помещение.

Помещения, в которых осуществляется обработка защищаемой информации должны обеспечивать сохранность информации, обрабатываемой на ОИ, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.

Машинные носители, содержащие информацию, обрабатываемую на ОИ, (диски, флеш-карты и т.д.) должны храниться в недоступном для посторонних лиц месте.

Помещения, в которых осуществляется обработка защищаемой информации, должны иметь входные двери и замки, гарантирующие закрытие помещений в нерабочее время.

Вскрытие и закрытие помещений, в которых ведется обработка защищаемой информации, производится работниками Учреждения, имеющими право доступа в соответствующее помещение.

Перед закрытием помещений, в которых осуществляется обработка защищаемой информации, по окончании рабочего дня работники, имеющие право доступа к защищаемой информации, обрабатываемым в соответствующем помещении, обязаны:

— убрать машинные носители, содержащие защищаемую информацию (диски, флеш-карты) в запираемые шкафы, запереть шкафы на замок;

— отключить ПК, а также ТС (кроме постоянно действующего оборудования) от сети, выключить освещение;

— закрыть окна, двери.

Перед открытием помещений, в которых осуществляется обработка защищаемой информации, работники обязаны:

— провести внешний осмотр с целью установления целостности двери и замка;

— открыть дверь и осмотреть помещение, проверить наличие и целостность замков на шкафах.

При обнаружении неисправности двери и запирающих устройств работники обязаны:

— не вскрывая помещение, в котором осуществляется обработка защищаемой информации, сообщить об этом руководителю;

— в присутствии не менее двух работников, включая руководителя, вскрыть помещение и осмотреть его;

— составить акт о выявленных нарушениях и передать установленным порядком руководителю.

Несанкционированное присутствие лиц, не имеющих права доступа к защищаемой информации, должно быть исключено.

Доступ в помещения, где осуществляется обработка защищаемой информации, вспомогательного и обслуживающего персонала (уборщиц, электромонтёров,

сантехников и других лиц) разрешается только в случае служебной необходимости в сопровождении лица, имеющего право доступа в соответствующее помещение, после принятия мер, исключающих визуальный просмотр документов, содержащих защищаемую информацию, обрабатываемую на ОИ, и экранов мониторов.

Внутренняя планировка и расположение рабочих мест в помещениях, где осуществляется обработка защищаемой информации, должны исключать визуальный просмотр обрабатываемой на ОИ защищаемой информации для работников, не осуществляющих обработку таких сведений. Окна помещений, в которых осуществляется обработка защищаемой информации, должны быть оборудованы шторами (жалюзи).

Ответственность за соблюдение порядка доступа в помещения, в которых осуществляется обработка защищаемой информации, возлагается на пользователей ОИ.

7.2. Требования к помещениям, предназначенным для размещения архивов

Помещения, предназначенные для размещения архивов, должны отвечать следующим требованиям:

— помещение должно располагаться в контролируемой зоне;

— желательно наличие видеокамеры системы видеозаписи, контролирующей вход в помещение;

— должны быть задействованы меры, исключающие неконтролируемое пребывание в помещении любых лиц, включая работников, не допущенных к работе с защищаемой информацией;

— помещение должно быть оборудовано датчиками пожарной и охранной сигнализации, желательно имеющими отдельные (не связанные с другими помещениями) шлейфы сигнализации, включенные в пульты охранно-пожарной сигнализации;

— помещение должно быть оборудовано средствами пожаротушения, желательно наличие автономной автоматической системы пожаротушения;

— помещение должно быть оборудовано необходимым количеством стеллажей и/или запираемых металлических шкафов для хранения архивных носителей;

— микроклимат (температурно-влажностный режим) помещения должен отвечать требованиям по сохранности архивных носителей, а условия хранения должны исключать возможность их повреждения (коробления, пересыхания, изгиба и вредного воздействия пыли, магнитных и электрических полей или ультрафиолета);

— помещение, предназначенное для хранения резервных копий, не должно совмещаться с помещением, в котором размещается оборудование, создающее и/или использующее указанные резервные копии.

7.3. Обеспечение безопасности серверного помещения

Для обеспечения безопасности серверного помещения необходимо оборудование его металлической дверью с замком. В конце рабочего дня помещение необходимо опечатывать. Также, необходимо оборудовать помещение техническими устройствами, сигнализирующими о несанкционированном доступе.

Доступ в серверное помещение осуществляется работниками отдела, в чьем ведении находится обеспечение работы информационной инфраструктуры Учреждения.

7.4. Порядок доступа работников и третьих лиц к обработке ПДн и в помещения, в которых осуществляется обработка

Доступ работников в помещения, в которых обрабатываются ПДн, осуществляется согласно: перечня помещений, в которых обрабатываются ПДн; перечня работников, допущенных к обработке ПДн.

Доступ третьих лиц в помещения, в которых обрабатываются ПДн, к обработке ПДн, или в серверную осуществляется в присутствии работника Учреждения.

8. Внутренний и внешний контроль соответствия обработки ПДн текущему законодательству и принятым локальным НПА

Внутренний и внешний контроль соответствия обработки ПДн текущему законодательству и принятым локальным НПА и другие мероприятия, целью которых является обеспечение информационной безопасности, проводятся в соответствии с Планом проведения внутренних мероприятий, который определяет периодичность проведения мероприятий по защите информации.

Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации состоит из следующих направлений:

— внешний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации;

— внутренний контроль соответствия обработки защищаемой информации требованиям к защите информации.

Внутренний контроль соответствия обработки защищаемой информации требованиям к защите персональных данных Учреждения состоит из контроля и надзора за исполнением требований по обработке и обеспечению безопасности информации.

8.1. Внешний контроль над соблюдением требований по обработке и обеспечению безопасности защищаемой информации

Внешний контроль и надзор за выполнением требований законодательства по обеспечению безопасности защищаемой информации, обрабатываемой на ОИ, осуществляется:

— Федеральной службой безопасности РФ в пределах своих полномочий;

— Федеральной службой по техническому и экспортному контролю в пределах своих полномочий;

— Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

8.2. Внутренний контроль соответствия обработки защищаемой информации требованиям к защите информации

8.2.1. Порядок внутреннего контроля соответствия обработки защищаемой информации требованиям к защите информации

1. Общие положения

Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите персональных данных в Учреждении (далее — Правила внутреннего контроля) разработаны с учетом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящие Правила внутреннего контроля определяют порядок осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в Учреждении.

Исполнение настоящих Правила внутреннего контроля обязательно для всех лиц, имеющих доступ к ПДн либо осуществляющих обработку ПДн в Учреждении, как

без использования средств автоматизации, так и в информационных системах ПДн Учреждения.

2. Порядок проведения внутренних проверок

Внутренний контроль соответствия обработки ПДн установленным требованиям к защите ПДн осуществляется Учреждением, являющимся оператором персональных данных, в форме проведения периодических (не реже одного раза в три года) внутренних проверок соответствия обработки ПДн требованиям к защите персональных данных в Учреждении.

Проверки осуществляются комиссией по контролю соответствия обработки ПДн требованиям к защите ПДн в Учреждении в составе, утверждаемом директором Учреждения.

Проверки могут проводиться в соответствии с отдельным поручением директора Учреждения или ответственного за организацию обработки ПДн.

Проверки осуществляются непосредственно на местах обработки ПДн путем опроса либо при необходимости путем осмотра рабочих мест лиц, допущенных к обработке ПДн в Учреждении, а также другими доступными способами.

Результаты проверок оформляются актом о результатах проведения внутренней проверки соответствия обработки ПДн требованиям к защите персональных данных в Учреждении, форма которого приведена в Приложении № 4.

3. Содержание проверок

В процессе проверки соответствия обработки ПДн без использования средств автоматизации требованиям к защите ПДн должно быть установлено:

— порядок и условия хранения бумажных носителей, содержащих персональные данные, обрабатываемые в Учреждении;

— условия доступа в помещения, где обрабатываются и хранятся бумажные носители с ПДн;

— наличие или отсутствие фактов несанкционированного доступа к персональным данным и необходимость принятия дополнительных мер по обеспечению безопасности ПДн;

— наличие или отсутствие фактов хранения носителей ПДн, подлежащих уничтожению в связи с истекшими сроками хранения либо наступлением других случаев, обозначенных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и текущим Положением по организации и проведению работ по обеспечению безопасности информации на объектах информатизации Учреждения.

При проведении проверки в ИСПДн должно быть установлено:

— соответствие используемых пользователями ИСПДн полномочий параметрам доступа;

— соблюдение пользователями ИСПДн правил парольной защиты;

— соблюдение пользователями ИСПДн правил антивирусной защиты;

— соблюдение пользователями ИСПДн правил работы со съемными носителями ПДн;

— соблюдение порядка доступа в помещения Учреждения, где расположены элементы ИСПДн;

— соблюдение порядка резервирования баз данных и хранения резервных копий;

— своевременность проведения мероприятий по уничтожению ПДн;

— знание пользователями ИСПДн своих действий во внештатных ситуациях;

— наличие или отсутствие фактов несанкционированного доступа к ИСПДн и необходимость принятия дополнительных мер по обеспечению безопасности ПДн;

— необходимость мероприятий по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Внутренний контроль соответствия обработки защищаемой информации требованиям к защите информации осуществляется ответственным за организацию обработки ПДн в Учреждении не реже 1 раза в 3 года. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, комиссией составляется акт о проведении внутреннего контроля. Администратор информационной безопасности докладывает руководству.

8.2.2. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

1. В данном подразделе определяется порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», и отражает соотношение указанного возможного вреда и мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством РФ.

2. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

1) Высокую в случаях:

— обработки сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;

— обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

— обработки персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации; обезличивания персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований, не предусмотренных пунктом 9 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; поручения

иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации;

— сбора персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.

2) Среднюю в случаях:

— распространения персональных данных на официальном сайте в информационно-телекоммуникационной сети "Интернет" оператора, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;

— обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;

— продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор;

— получения согласия на обработку персональных данных посредством реализации на официальном сайте в информационно-телекоммуникационной сети "Интернет" функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;

— осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

3) Низкую в случаях:

— ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Закона о персональных данных;

— назначения в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником оператора.

3. Результаты оценки вреда оформляются актом оценки вреда.

4. Акт оценки вреда должен содержать:

а) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;

б) дату издания акта оценки вреда;

в) дату проведения оценки вреда;

г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;

д) степень вреда, которая может быть причинена субъекту персональных данных, в соответствии с пунктами 1-3 пункта 8.2.2.

5. Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

6. В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии с пунктами 1-3 пункта 8.2.2. могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

9. Порядок проведения служебной проверки по фактам нарушения требований по обеспечению безопасности защищаемой информации

9.1. Классификация нарушений требований по обеспечению безопасности защищаемой информации

Нарушения требований по обеспечению безопасности защищаемой информации, обрабатываемой в ИС, и их последствия классифицируются по значимости на:

— нарушения I категории;
— нарушения II категории;
— нарушения III категории.

Служебная проверка назначается по нарушениям I и II категорий.

9.2. Перечень нарушений требований по обеспечению безопасности защищаемой информации

Нарушения I категории, к которым относятся нарушения, повлекшие за собой разглашение (утечку), уничтожение (искажение) защищаемой информации и/или утрату машинных носителей защищаемой информации, выведение из строя технических и программных средств, входящих в состав ОИ, а именно:

— успешный подбор административного пароля;
— несанкционированная реконфигурация параметров ОИ;
— утрата или кража резервной копии базы, содержащей защищаемую информацию;
— необоснованная передача информационных массивов ОИ;
— организация утечки сведений по техническим каналам;
— умышленное нарушение работоспособности ОИ;
— НСД к защищаемой информации;
— несанкционированное внесение изменений в ОИ;
— умышленное заражение ОИ вредоносным программным обеспечением (далее — ПО);
— проведение работ на ОИ, повлекших за собой необратимую потерю данных;
— другие действия, попадающие под действия статей, приведенных в таблице 1.

Таблица 1

Номер статьи	Название статьи
1	2
Федеральный закон РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»	
ст. 17	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
Федеральный закон РФ № 152-ФЗ от 27 июля 2006 г. «О персональных данных»	
ст. 24	Ответственность за нарушение требований настоящего Федерального закона

Номер статьи	Название статьи
1	2
Кодекс РФ об административных правонарушениях	
ст. 5.39	Отказ в предоставлении информации
ст. 13.11	Нарушение законодательства Российской Федерации в области персональных данных
ст. 13.11.1	Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера
ст. 13.12	Нарушение правил защиты информации
ст. 13.14	Разглашение информации с ограниченным доступом
ст. 19.7	Непредставление сведений (информации)
Уголовный кодекс РФ	
ст. 137	Нарушение неприкосновенности частной жизни
ст. 140	Отказ в предоставлении гражданину информации
ст. 272	Неправомерный доступ к компьютерной информации
ст. 273	Создание, использование и распространение вредоносных компьютерных программ
ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
Трудовой кодекс РФ	
ст. 90	Ответственность за нарушение норм, регулирующих обработку и защиту ПДн работника

Нарушения II категории, к которым относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке), уничтожению (искажению) защищаемой информации, утрате машинных носителей защищаемой информации, выведению из строя технических и программных средств, входящих в состав ОИ, а именно:

— ошибка при доступе к информационным ресурсам ОИ (набор не назначенного пароля, более 3 (трех) раз подряд, периодически);

— оставление ОИ включенным (незаблокированным) во время отсутствия на рабочем месте;

— перезагрузка ОИ при сбоях в работе, в т.ч. аварийная (неоднократная) перезагрузка путем нажатия кнопки RESET;

— утрата учтенного машинного носителя информации;

— многократная неудачная попытка входа под чужим именем, паролем;

— удачная попытка входа под чужим именем, паролем;

— несанкционированная очистка журналов аудита;

— несанкционированное копирование защищаемой информации на внешние носители информации;

— несанкционированная установка (удаление) ПО в ИС;

— несанкционированное изменение конфигурации ПО ИС;

— попытка получения прав администратора для доступа к информационным ресурсам ОИ (увеличения полномочий собственных прав, получение прав на отладку программ) удачная и неудачная;

— попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная;

— неумышленное заражение ОИ вредоносным ПО;

— несанкционированное использование сканирующего ПО;

— несанкционированное использование анализаторов протоколов (снифферов);

— несанкционированный просмотр защищаемой информации, вывод на печать и т.п.

Нарушения III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:

— ошибка при доступе к информационным ресурсам ОИ (набор неправильного пароля, сетевого имени более 3 (Трех) раз подряд, не периодическая);

— периодическая попытка неудачного доступа защищаемой информации, обрабатываемой на ОИ;

— перевод времени на ОИ;

— однократная перезагрузка ОИ при сбоях в работе ОИ, в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;

— нецелевое использование корпоративных ресурсов (печать, доступ в сеть международного информационного обмена Интернет, электронная почта и т.п.).

9.3. Назначение и проведение служебной проверки

Служебная проверка назначается по нарушениям I и II категорий.

Служебная проверка может быть инициирована на основании устного заявления, докладной или служебной записки любого работника по выявленному отдельному факту нарушения, либо по факту группы нарушений.

Служебная проверка проводится комиссией, состав которой утверждает руководитель Учреждения.

В случае необходимости Председатель комиссии может привлекать к работе:

— непосредственного начальника нарушителя;

— экспертов из других подразделений;

— специалистов организаций-лицензиатов ФСТЭК России и ФСБ РФ.

Члены комиссии имеют право:

— требовать документального подтверждения факта нарушений информационной безопасности;

— устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству РФ;

— брать письменные объяснения по поводу выявленных нарушений у любого работника Учреждения.

За выявление и классификацию нарушения требований по обеспечению безопасности защищаемой информации, требующего проведения процедуры служебной проверки, ответственность несет администратор информационной безопасности.

9.4. Оформление результатов работы комиссии

Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения на имя руководителя Учреждения с предложениями по необходимым организационным выводам, а также по расширению или дополнению

перечня нарушений требований по обеспечению безопасности защищаемой информации.

Результатом работы Комиссии должен стать Акт, форма которого приведена в Приложении № 7, в котором изложены:

— состав комиссии;

— период времени, в течение которого проводилась служебная проверка;

— основание для проведения служебной проверки;

— документальное подтверждение фактов нарушений, выявленных в ходе служебной проверки и имеющих значение в определении наличия нарушений, а также иных фактов, которые могут привести к нарушению конфиденциальности информации;

— установленные причины выявленных нарушений;

— вывод о значимости, их причинах и виновных, допустивших данные нарушения;

— сформированные предложения по устранению причин выявленных нарушений;

— рекомендации по совершенствованию обеспечения безопасности защищаемой информации, исключающие в дальнейшем подобные нарушения.

10. Порядок приостановления обработки защищаемой информации

При обнаружении нарушений I категории обработка защищаемой информации незамедлительно приостанавливается в той части ОИ, которая подвержена влиянию факта нарушения информационной безопасности, до выявления причин нарушений и устранения этих причин.

По факту нарушения требований по обеспечению безопасности, повлекшего приостановление обработки защищаемой информации, проводится служебная проверка.

11. Обезличивание ПДн

11.1. Условия обезличивания ПДн

В соответствии с [2] обезличивание ПДн может быть проведено:

— если обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением таких целей как продвижение товаров, работ и услуг на рынке, политической агитации;

— по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Обезличивание ПДн осуществляется с учетом [6].

11.2. Методы обезличивания ПДн

Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки ПДн. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

— метод введения идентификаторов (замена части сведений (значений ПДн) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

— метод изменения состава или семантики (изменение состава или семантики ПДн путем замены результатами статистической обработки, обобщения или удаления части сведений);

— метод декомпозиции (разбиение множества (массива) ПДн на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

— метод перемешивания (перестановка отдельных записей, а также групп записей в массиве ПДн).

11.3. Процедура обезличивания

Процедура обезличивания обеспечивает практическую реализацию метода обезличивания и задается своим описанием.

Допускается программная реализация процедуры различными способами и средствами.

11.4. Организация обработки ПДн и обезличенных данных

При использовании процедуры обезличивания не допускается совместное хранение ПДн и обезличенных данных.

Обезличивание ПДн субъектов должно производиться перед внесением их на ОИ.

Учреждение вправе обрабатывать на ОИ обезличенные данные, полученные от третьих лиц.

В процессе обработки обезличенных данных, при необходимости, может проводиться деобезличивание. После обработки ПДн, полученные в результате такого деобезличивания, уничтожаются.

Обработка ПДн до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с действующим законодательством РФ с применением мер по обеспечению безопасности ПДн.

Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

Хранение и защиту дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, следует обеспечить в соответствии с внутренними процедурами обеспечения конфиденциальности, установленными в Учреждении. При этом должно обеспечиваться исполнение установленных правил доступа пользователей к хранимым данным, резервного копирования и возможности актуализации и восстановления хранимых данных.

Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки ПДн как их неотъемлемый элемент, а также максимально эффективно использовать имеющуюся у Учреждения инфраструктуру, обеспечивающую обработку ПДн.

11.5. Рекомендации по выбору методов обезличивания в соответствии с классом задач обработки

При выборе методов и процедур обезличивания ПДн следует руководствоваться целями и задачами обработки ПДн.

Обезличивание ПДн, обработка которых осуществляется с разными целями, может осуществляться разными методами.

Возможно объединение различных методов обезличивания в одну процедуру.

Для решения каждой задачи обработки определяются требуемые свойства обезличенных данных и метода обезличивания, которые зависят от набора действий, осуществляемых с ПДн (сбор, хранение, изменение, систематизация, осуществление выборки, поиск, передача и т.д.) в соответствии с принципом разумной достаточности (определяется минимально необходимый перечень свойств). Целесообразно предусмотреть возможность обработки обезличенных данных без предварительного деобезличивания.

При выборе метода и процедуры обезличивания также следует учитывать:

— объем ПДн, подлежащих обезличиванию (некоторые методы неэффективны на малых объемах);

— форму представления данных (отдельные записи, файлы, таблицы баз данных и т.д.);

— область обработки обезличенных данных (необходим ли другим операторам доступ к обезличиваемым данным);

— способы хранения обезличенных данных (локальное хранение, распределенное хранение и т.д.);

— применяемые в информационной системе меры по обеспечению безопасности данных.

Ниже представлены типовые классы задач, состоящие из наиболее часто встречающихся задач обработки ПДн. Проведенная классификация позволяет в Учреждении применять наиболее эффективные для данного класса методы.

В Таблице 2 приведены рекомендации по выбору метода обезличивания в зависимости от класса решаемых задач. Рекомендованные методы ранжированы в порядке убывания эффективности их применения.

Таблица 2 — Рекомендации по выбору метода обезличивания

Класс задач	Задачи обработки	Метод обезличивания
1	2	3
Статистическая обработка и статистические исследования ПД	– осуществление выборки по заявленным параметрам; – проведение исследований по заданным параметрам субъектов.	– метод перемешивания; – метод декомпозиции; – метод изменения состава или семантики.
Сбор и хранение ПД	– внесение персональных данных субъектов в информационную систему на основе анкет, заявлений и прочих документов.	– метод декомпозиции; – метод перемешивания; – метод введения идентификаторов.
Обработка поисковых запросов (поиск данных о субъектах и поиск субъектов по известным данным)	– поиск информации о субъектах; – печать и выдача субъектам документов в установленной форме, содержащих ПДн; – выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов.	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.
Актуализация ПД	– внесение изменений в существующие записи о субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; – внесение изменений в существующие записи о субъектах на основе исследований, выполнения органом своих функций или требований законодательства РФ.	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.
Интеграция данных различных операторов	– поиск информации о субъектах; – передача данных смежным органам.	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.
Ведение учета субъектов ПД	– прием анкет, заявлений; – ведение учета ПДн в соответствии с функциями органа.	– метод декомпозиции; – метод перемешивания; – метод введения идентификаторов.

При наличии в системе нескольких классов задач рекомендуется выбирать общий метод для всех этих классов, либо совместно применять несколько методов.

12. Уничтожение защищаемой информации, в том числе машинных носителей

12.1. Условия уничтожения защищаемой информации

Уничтожение защищаемой информации должно быть проведено:

— по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством;

— в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн;

— в случае выявления фактов неправомерной обработки ПДн (в том числе при обращении субъекта ПДн) и обеспечить их правомерность не предоставляется возможным.

12.2. Порядок уничтожения защищаемой информации

Перед уничтожением защищаемой информации необходимо:

— убедиться в правовых основаниях уничтожения защищаемой информации;

— убедиться в том, что уничтожается именно та защищаемая информация, которая предназначена для уничтожения;

— проверить необходимость уведомления об уничтожении ПДн субъекта ПДн, или его представителя, или третьих лиц в предусмотренном случае.

12.3. Способы уничтожения защищаемой информации

Уничтожение защищаемой информации возможно осуществить одним из следующих способов:

— физическое уничтожение носителя защищаемой информации;

— уничтожение защищаемой информации с носителя защищаемой информации.

Для физического уничтожения бумажного носителя защищаемой информации используются два вида уничтожения — уничтожение через шредирование (измельчение и гидрообработка) и уничтожение через термическую обработку (сжигание).

Уничтожение информации на машинных носителях необходимо осуществлять путем стирания информации с использованием программного обеспечения с гарантированным уничтожением. При уничтожении защищаемой информации необходимо учитывать возможность их наличия в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством РФ.

Если защищаемая информация хранятся на машинном носителе, пришедшем в негодность, отслужившем установленный срок или утратившем практическое значение, такой машинный носитель подлежит физическому уничтожению. Перед уничтожением машинного носителя на нем производится стирание защищаемой информации путем использования программного обеспечения с гарантированным уничтожением информации.

После стирания защищаемой информации машинный носитель уничтожается одним из следующих способов: разрезание, сжигание, механическое уничтожение,

сдача предприятию по утилизации вторичного сырья или иными методами, исключающими возможность восстановления содержания защищаемой информации.

По факту уничтожения машинных носителей информации работниками ответственного структурного подразделения составляется соответствующий Акт, формы которых приведены в Приложении № 1 к настоящему Положению.

12.4. Подтверждение уничтожения персональных данных

12.4.1. В случае если обработка персональных данных осуществляется Учреждением без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

12.4.2. В случае если обработка персональных данных осуществляется Учреждением с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, содержащимся в пунктах 12.4.3 и 12.4.4, и выгрузка из журнала регистрации событий в ИСПДн (далее - выгрузка из журнала).

12.4.3. Акт об уничтожении персональных данных, форма которого приведена в Приложении № 8, должен содержать:

а) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес оператора;

б) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению оператора (если обработка была поручена такому (таким) лицу (лицам);

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

12.4.4. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с Федеральным законом РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи», признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в пункте «г» пункта 12.4.4.

12.4.5. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

12.4.6. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 12.4.5, недостающие сведения вносятся в акт об уничтожении персональных данных.

12.4.7. В случае если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, установленным пунктами 12.4.3 и 12.4.4, и выгрузка из журнала, соответствующая требованиям, установленным пунктом 12.5.5.

12.4.8. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

13. Порядок управления доступом субъектов доступа к объектам доступа ОИ

Предоставление доступа пользователю к ОИ (или изменение прав доступа) осуществляется на основании Перечня лиц, допущенных к обработке ПДн, утвержденного руководителем Учреждения.

Назначение прав доступа пользователей к защищаемой информации (ПДн), обрабатываемой на ОИ, осуществляется путем внесения работника в Перечень лиц, допущенных к обработке ПДн, утвержденного руководителем Учреждения.

Контроль за деятельностью пользователей ОИ ведется администратором информационной безопасности.

Наличие у работника избыточных, неконтролируемых прав доступа является нарушением требований по обеспечению безопасности информации, обрабатываемой на ОИ.

Основанием для прекращения права доступа пользователя к ОИ, может служить его исключение из утвержденного руководителем регламентирующего локального НПА.

14. Организация парольной защиты на ОИ

14.1. Общие положения

Целью применения и реализации парольной защиты является исключение утечки защищаемой информации, обрабатываемой на ОИ, а также ее несанкционированной модификации или уничтожения.

Правила парольной защиты регламентируют организационно-техническое обеспечение процессов выдачи, смены и прекращения действия паролей на ОИ, а также контроль над действиями пользователей ОИ при работе с паролями.

Организационное и техническое обеспечение процессов выдачи, использования, смены и прекращения действия паролей во всех подсистемах ОИ и контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности.

14.2. Порядок организации парольной защиты

Защите паролем подлежит доступ к следующей информации:

— базовая система ввода-вывода ОИ;
— настройки ОС;
— настройки сетевого оборудования;
— настройки СЗИ;
— ПО, предназначенное для обработки защищаемой информации;
— ресурсы ОИ и информационные ресурсы, содержащие защищаемую информацию.

Личные пароли доступа пользователей ОИ генерируются и распределяются централизованно уполномоченным работником, однако, после пользователь должен поменять пароль самостоятельно с учетом следующих требований:

— длина пароля должна быть не менее 8 (восьми) символов;

— в числе символов пароля, обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, а также цифры и символы;

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования автоматизированных рабочих мест, общепринятые сокращения (например, ЭВМ, ЛВС, USER, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе ОИ;

— не допускается использование в качестве пароля одного и того же повторяющегося символа или повторяющейся комбинации из нескольких символов;

— не допускается использование в качестве пароля комбинации символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

— при смене пароля новое значение должно отличаться от предыдущего;

— не допускается использование ранее использованных паролей.

Лица, использующие паролирование, обязаны:

— четко знать и строго выполнять требования по парольной защите;

— своевременно сообщать администратору информационной безопасности обо всех нештатных ситуациях, возникающих при работе с паролями.

При организации парольной защиты запрещается:

— записывать свои пароли в очевидных местах (например, на мониторе, на обратной стороне клавиатуры и т.д.);

— хранить пароли в записанном виде на отдельных листах бумаги;

— сообщать другим лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

14.3. Порядок применения парольной защиты

Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя должна производиться в следующих случаях:

— при подозрении на компрометацию пароля;

— по завершении срока действия пароля;

— в случае прекращения полномочий пользователя (увольнение, переход на другую работу внутри организации) — после завершения последнего сеанса работы данного пользователя с системой;

— по указанию администратора информационной безопасности;

— каждые 6 месяцев;

— в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) администратора информационной безопасности.

Для предотвращения доступа к ОИ, пользователь ОИ во время перерыва в работе обязан осуществить блокирование системы. Для этого необходимо нажать одновременно комбинацию клавиш <Windows><L> (для ОС семейства Windows); для ОС семейства Linux необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><L> или <Windows><L>.

Порядок применения (смены) паролей при работе на ОИ, оборудованных системой защиты, приведен в эксплуатационной документации на СЗИ.

Ответственность за организацию парольной защиты возлагается на администратора информационной безопасности.

Ответственность за соблюдение требований парольной защиты возлагается на администратора информационной безопасности и пользователей ОИ в пределах полномочий.

Нарушения организации и порядка применения парольной защиты классифицируются в соответствии с п. 9.2 Положения, обрабатываемой на ОИ. При выявлении нарушений I и II категории проводится служебная проверка в соответствии с п. 9 Положения.

В случае несоответствия данной парольной политики технической документации по СКЗИ, то применять следует требования технической документации по СКЗИ.

15. Организация антивирусной защиты на ОИ

15.1. Общие положения

Целью антивирусной защиты ОИ является предотвращение и нейтрализация негативных воздействий вредоносного ПО на информационные ресурсы, содержащие защищаемую информацию, и ПО, предназначенное для обработки такой информации.

Порядок организации антивирусной защиты определяет требования к организации защиты ОИ от разрушающего воздействия вредоносного ПО и устанавливают ответственность за их выполнение.

К использованию на ОИ допускаются только лицензионные и сертифицированные ФСТЭК России и ФСБ РФ по требованиям безопасности информации средства антивирусной защиты.

Установка и начальная настройка средств антивирусной защиты на ОИ может осуществляться администратором информационной безопасности, а также представителями организации-лицензиата ФСТЭК России и ФСБ РФ.

Обновления сигнатур средств защиты от вредоносного ПО и контроль их работоспособности производится в автоматическом режиме.

Пользователи ИС, обязаны руководствоваться в работе Порядком организации антивирусной защиты.

15.2. Порядок организации антивирусной защиты

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), защищаемая информация, обрабатываемая на ОИ, и содержащаяся на машинных носителях (жесткие магнитные диски, оптические носители информации (*CD-, DVD*-диски), флеш-накопители *USB*). Антивирусный контроль информации необходимо осуществлять перед архивированием или записью на машинный носитель. Файлы, помещаемые в электронный архив, в обязательном порядке проходят антивирусный контроль.

Устанавливаемое (изменяемое) ПО должно быть предварительно проверено на отсутствие вредоносного ПО. После установки (изменения) ПО должна быть осуществлена антивирусная проверка ОИ.

При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.)

пользователь ОИ самостоятельно (или совместно с администратором информационной безопасности), должен провести внеочередной антивирусный контроль ОИ.

В случае обнаружения вредоносного ПО при проведении антивирусной проверки пользователь ОИ обязан:

— приостановить работу ОИ;

— немедленно поставить в известность о факте обнаружения вредоносного ПО администратора информационной безопасности, а также других пользователей ОИ, использующих зараженные файлы в работе;

— совместно с владельцем зараженных вредоносным ПО файлов провести анализ возможности их дальнейшего использования;

— провести «лечение» или удаление зараженных файлов.

При включении ПК установленное антивирусное ПО должно производить сканирование в фоновом режиме.

Ответственность за проведение мероприятий антивирусной защиты и контроля, соблюдения требований антивирусной защиты на ОИ возлагается на администратора информационной безопасности.

16. Организация учета и хранения машинных носителей информации

16.1. Порядок учета машинных носителей информации

Все машинные носители информации, содержащие защищаемую информацию, а именно:

— жесткие диски, SSD находящиеся в корпусах ОИ;

— жесткие диски, SSD находящиеся во внешних RAID-массивах серверов;

— кассеты со стриммерными лентами, находящиеся в стриммерных устройствах;

— USB-носители, находящиеся у пользователей ОИ, и содержащие резервные копии защищаемой информации;

— CD-R, CD-RW, DVD-R и/или DVD-RW-носители,

подлежат регистрации и учету.

Учетный номер машинного носителя информации должен наноситься непосредственно на корпус носителя и быть нестираемым.

На рабочих местах пользователей ОИ не должны находиться неучтенные машинные носители информации, содержащие защищаемую информацию.

Запрещается копирование защищаемой информации пользователями ОИ с целью их передачи другим работникам или посторонним лицам.

Работник, получивший носитель для работы с защищаемой информацией, обязан обеспечить его недоступность для третьих лиц (посторонних лиц и работников, не имеющих допуск к защищаемой информации).

Полученные извне машинные носители информации должны:

— проверяться на наличие вредоносных программных продуктов;

— учитываться в соответствии с настоящей политикой;

— передаваться работникам, являющимся пользователями ОИ, только с разрешения руководителя структурного подразделения с записью в соответствующих формах учета.

Регистрацию и учет машинных носителей информации, содержащих информацию, обрабатываемую на ОИ, осуществляет администратор информационной

безопасности в соответствующем журнале учета машинных носителей информации, форма которого приведена в Приложении № 2 к настоящему Положению.

На каждый машинный носитель должен быть нанесен учетный номер, который также указан в журнале учета машинных носителей информации. Наносить учетный номер можно как на корпус машинного носителя, так и на бирку.

16.2. Порядок хранения машинных носителей информации

Хранение машинных носителей информации осуществляется в условиях, исключающих утрату их функциональности и хранимой информации, а также НСД к информации.

Машинные носители информации должны храниться в недоступном для посторонних лиц месте.

16.3. Порядок эксплуатации машинных носителей информации

Выдача машинных носителей информации пользователям ОИ производится администратором информационной безопасности под подпись в соответствующем журнале учета машинных носителей информации.

Передача машинных носителей информации для ремонта или утилизации запрещена.

Все машинные носители информации, потерявшие актуальность, передаются администратору информационной безопасности. По факту уничтожения машинного носителя информации в журнале учета машинных носителей информации администратором информационной безопасности производится отметка об уничтожении и составляется акт об уничтожении, приведенный в приложении №3.

17. Организация резервирования и восстановления информации на ОИ

17.1. Общие положения

С целью обеспечения возможности незамедлительного восстановления защищаемой информации на ОИ, модифицированных или уничтоженных вследствие НСД к ним или возникновении нештатных ситуаций, повлекших за собой потерю данных, организуется резервирование и восстановление информации на ОИ, а также работоспособности ОИ.

17.2. Информация, подлежащая резервному копированию

Резервному копированию подлежат следующие информационные ресурсы:

— файлы, каталоги, БД, содержащие информацию, обрабатываемую на ОИ;
— системные и конфигурационные файлы общесистемного и прикладного ПО;
— конфигурационные файлы сетевого оборудования;
— системные и конфигурационные файлы СЗИ.

17.3. Порядок резервирования и хранения резервных копий

Резервное копирование защищаемой информации, обрабатываемой на ОИ, должно осуществляться регулярно на машинные носители информации, создавая тем самым резервный электронный архив.

Перед резервным копированием машинный носитель информации (жесткий магнитный диск, оптический носитель информации (CD-, DVD-диск), флеш-накопитель USB) проверяется на отсутствие вредоносного ПО. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Качество записи резервных копий на машинных носителях информации должно проверяться непосредственно после изготовления копии.

Надежность и правильность записи критической информации следует периодически проверять использованием контрольных процедур восстановления.

17.4. Порядок восстановления работоспособности ОИ

В случае возникновения нештатной ситуации, вызвавшей полную или частичную потерю работоспособности ОИ, должно быть обеспечено ее восстановление из резервной копии. Факт возникновения нештатной ситуации на ОИ подлежит обязательной регистрации работниками отдела по обеспечению безопасности деятельности в журнале учета нештатных ситуаций в информационных системах, форма которого приведена в Приложении № 3 к настоящему Положению.

При восстановлении работоспособности ПО сначала осуществляется резервное копирование информационных ресурсов, содержащих защищаемую информацию, затем производится полное уничтожение некорректно работающего ПО.

Восстановление ПО производится путем его установки с использованием эталонных дистрибутивов (установочных дисков).

При работе в ИС рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения ТС, входящих в состав ИС, и (или) защищаемой информации, обрабатываемой в ИС, в результате сбоев в сети электропитания.

Восстановление СЗИ производится с использованием дистрибутива. При восстановлении работоспособности СЗИ необходимо выполнить их настройку в соответствии с требованиями безопасности информации. После настройки СЗИ выполняется резервное копирование настроек данных СЗИ с помощью встроенных в них функций на учтенный машинный носитель информации.

Ответственность за организацию резервного копирования, проведения мероприятий по восстановлению работоспособности информационных ресурсов, технических и программных средств, входящих в состав ОИ, возлагается на администратора информационной безопасности.

18. Порядок работы с электронными журналами протоколирования и анализа (аудита) значимых событий

Правила и порядок протоколирования и анализа (аудита) значимых событий в ИС направлены на превентивную фиксацию и изучение действий субъектов доступа на ОИ, а также на своевременное выявление фактов НСД к защищаемой информации.

Все события, происходящие в общесистемном, прикладном ПО, других критических приложениях и СЗИ, применяемых на ОИ должны протоколироваться в специальные электронные журналы аудита.

Проверке подлежат следующие электронные журналы:

— Журналы, формируемые ОС и прикладным ПО;

— Журнал событий, формируемых СУБД;

— Журнал событий, формируемых СЗИ.

На ОИ, на которых установлены СЗИ от НСД, проверка соответствующего электронного журнала событий, формируемых данными СЗИ, производится в соответствии с прилагаемой к ним технической и эксплуатационной документацией.

19. Порядок обращения со средствами защиты информации

19.1. Учет средств защиты информации

Под СЗИ в настоящем разделе понимается СЗИ, не являющееся средствами криптографической защиты.

Процедура установки СЗИ сопровождается оформлением акта установки СЗИ работниками отдела по обеспечению безопасности деятельности, форма которого приведена в Приложении № 5 к настоящему Положению. Процедура деинсталляции СЗИ сопровождается оформлением акта деинсталляции СЗИ, форма которого приведена в Приложении № 6 к настоящему Положению.

19.2. Уничтожение средств защиты информации

Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

19.3. Ответственность за нарушение требований эксплуатации средств защиты

Контроль за организацией и обеспечением функционирования СЗИ возлагается на администратора информационной безопасности в пределах его полномочий.

Пользователи ОИ несут персональную ответственность за:

— эксплуатацию установленных на ОИ СЗИ;

— соблюдение положений настоящего Положения.

Администратор информационной безопасности несет ответственность за:

— сохранность полученных СЗИ;

— соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки защищаемой информации с использованием СЗИ лицензионным требованиям и условиям, эксплуатационной и технической документации к СЗИ.

20. Порядок обеспечения информационной безопасности ИС при модернизации (обновлении) аппаратных и программных компонентов

Настоящие правила и порядок модернизации (обновления) аппаратных компонентов, ПО ОИ в целях информационной безопасности направлены на защиту ресурсов от:

— нарушения штатной работы информационных ресурсов и сервисов;
— нарушения штатного функционирования оборудования;
— несанкционированной модификации;
— несанкционированного копирования.

Ответственность за невыполнение требований настоящего пункта, проведение в плановом порядке работ по обновлению оборудования, ОС, ПО в целях своевременной ликвидации выявленных уязвимостей ПО в информационной инфраструктуре, за отслеживание появления новых уязвимостей в используемых ОС, за установку патчей, устраняющих данные уязвимости, за тестирование ОИ при внесении изменений и дополнений в ПО и оборудование на отсутствие негативных воздействий на функционирование ОИ, ответственность за мониторинг событий, фиксируемых системами безопасности, несет администратор информационной безопасности.

Установке нового оборудования предшествует тестирование ОИ на отсутствие негативных воздействий вновь устанавливаемого оборудования.

Установке обновлений предшествует тестирование ОИ на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

При обнаружении негативного воздействия устанавливаемого оборудования на ОИ, функционирующие в штатном режиме, такое оборудование не устанавливается. В этом случае разрабатывается план дополнительных мероприятий, направленных на устранение негативного воздействия устанавливаемого оборудования.

Установке новых версий ПО или внесению изменений и дополнений в действующее ПО предшествует тестирование ОИ на отсутствие негативных воздействий устанавливаемого ПО.

Установка протестированного оборудования и (или) патчей, новых версий ПО или внесение изменений и дополнений в действующее ПО, применение организационно-технических и (или) аппаратно-программных решений может быть произведено на основании решения администратора информационной безопасности.

Тестирование нового оборудования и обновлений ПО не должно осуществляться на ресурсах действующей информационной инфраструктуры ИС.

21. Контроль и надзор за эксплуатацией аттестованных ОИ

Государственный контроль и надзор за проведением аттестации ОИ по требованиям безопасности информации, а также за соблюдением правил эксплуатации, аттестованных ОИ и эффективностью принятых мер защиты некриптографическими методами, проводится ФСТЭК России и ее территориальными органами.

Объем, содержание и порядок государственного контроля и надзора устанавливаются нормативными и методическими документами по обеспечению безопасности информации при ее обработке на ОИ. Контрольные мероприятия проводятся в соответствии с утвержденными планами работ.

Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации ОИ, проверку правильности оформления отчетных документов и протоколов аттестационных испытаний, проверку своевременности внесения изменений в организационно-распорядительные документы по обеспечению безопасности информации, а также контроль за эксплуатацией аттестованных ОИ.

22. Порядок действий работников в нештатных ситуациях

В случае наличия нештатной ситуации порядок действий, который не регламентируется настоящим Положением, администратором ИБ вырабатывается конкретный план действий с учетом текущей ситуации.

Нештатными (кризисными) ситуациями являются:

1) Разглашение информации, подлежащих защите в Учреждения, работниками, имеющими к ней право доступа, в том числе:

— разглашение информации лицам, не имеющим права доступа к защищаемой информации;

— передача информации по открытым линиям связи;

— обработка защищаемой информации на незащищенных технических средствах обработки информации;

— опубликование защищаемой информации в открытой печати и других средствах массовой информации в случаях, не предусмотренных законодательством Российской Федерации;

— передача носителя защищенной информации лицу, не имеющему права доступа к ней;

— утрата носителя с защищаемой информацией.

2) Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

— несанкционированное изменение информации;

— несанкционированное уничтожение информации

— несанкционированное копирование информации.

3) Несанкционированный доступ к защищаемой информации:

— подключение технических средств к средствам и системам объекта информатизации;

— маскировка под зарегистрированного пользователя;

— использование дефектов программного обеспечения объекта информатизации (ОИ);

— использование программных закладок;

— применение программных вирусов;

— хищение носителя защищаемой информации;

— нарушение функционирования технических средств (ТС) обработки информации;

4) Дефекты, сбои, отказы, аварии ТС и систем ОИ.

5) Дефекты, сбои и отказы программного обеспечения ОИ.

6) Сбои, отказы и аварии систем обеспечения ОИ.

7) Природные явления, стихийные бедствия:

— термические, климатические факторы (пожары, наводнения и т. д.);

— механические факторы (землетрясения и т. д.);

— электромагнитные факторы (грозовые разряды и т. д.).

Порядок действий при обнаружении нештатных ситуаций в Учреждении представлен в таблице 3.

Таблица 3. Порядок действий при обнаружении нештатных ситуаций в Учреждении.

Нештатная ситуация	**Оценка ситуации**	**Действия персонала**
Разглашение защищаемой информации работниками, имеющими к ней доступ	Обнаружился случившийся факт	1. Работник Учреждения сообщает об инциденте руководителю. 2. Проводится служебная проверка и принимается соответствующее решение.
	Производится в текущий момент	1. Работник прерывает несанкционированный процесс. 2. Работник сообщает об инциденте руководителю. 3. Проводится служебная проверка и принимается соответствующее решение.
Неправомерные действий со стороны лиц, имеющих право доступа к защищаемой информации/ Несанкционированное копирование, изменение, уничтожение защищаемой информации	Обнаружился случившийся факт	1. Администратор ИБ блокирует доступ к ИСПДн. 2. Руководитель совместно с Администратором ИБ предпринимает действия по сбору и обеспечению сохранности улик. 3. Проводится служебная проверка и принимается соответствующее решение.
	Производится в текущий момент	1. Администратор ИБ прерывает несанкционированный процесс. 2. Администратор ИБ блокирует доступ к ИСПДн. 3. Руководитель совместно с Администратором ИБ предпринимает действия по сбору и обеспечению сохранности улик. 4. Проводится служебная проверка и принимается соответствующее решение.
НСД к защищаемой информации/ Подключение сторонних технических средств к средствам системы объекта информатизации	Обнаружился случившийся факт	1. Администратор ИБ блокирует доступ к ИСПДн для нарушителя. 2. Администратор ИБ сообщает об инциденте руководителю. 3. Проводится служебная проверка и принимается соответствующее решение.
	Производится в текущий момент	1. Администратор ИБ прерывает процесс работы нарушителя. 2. Администратор ИБ блокирует доступ к ИСПДн для нарушителя. 3. Администратор ИБ сообщает об инциденте руководителю. 4. Проводится служебная проверка и принимается соответствующее решение.

НСД к защищаемой информации/ Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент	1. Администратор ИБ прерывает процесс работы нарушителя. 2. Администратор ИБ предпринимает действия для задержания нарушителя (вызывает полицию). 3. Администратор ИБ сообщает об инциденте руководителю. 4. Проводится служебная проверка и принимается соответствующее решение.
	Внутренним злоумышленником, либо производилась в прошлом	1. Администратор ИБ прерывает процесс работы нарушителя. 2. Администратор ИБ сообщает об инциденте руководителю. 3. Проводится служебная проверка и принимается соответствующее решение.
НСД к защищаемой информации/ Использование дефектов ПО ОИ	Внешним злоумышленником в текущий момент/ Внутренним злоумышленником, либо производилась в прошлом	1. Администратор ИБ прерывает процесс работы нарушителя. 2. Администратор ИБ блокирует доступ к ИСПДн. 3. Администратор ИБ сообщает об инциденте руководителю. 4. Проводится служебная проверка и принимается соответствующее решение.
НСД к защищаемой информации/ Использование программных закладок	Внешним злоумышленником в текущий момент/ Внутренним злоумышленником, либо производилась в прошлом	1. Администратор ИБ прерывает процесс работы нарушителя. 2. Администратор ИБ блокирует доступ к ИСПДн. 3. Администратор ИБ определяет возможный ущерб, нанесённый программной закладкой. 4. Администратор ИБ сообщает об инциденте руководителю. 5. Производится служебная проверка и принимается соответствующее решение.
Обнаружение программных вирусов		1. Администратор ИБ прерывает процесс работы ИСПДн. 2. Администратор ИБ определяет возможный ущерб, нанесенный программно-математическим воздействием. 3. Администратор ИБ проводит контроль ИСПДн в соответствии с инструкцией по организации антивирусной защиты. 4. Администратор ИБ составляет акт об инциденте.
Хищение носителя защищаемой информации		1. Проводится служебная проверка и принимается соответствующее решение.
Нарушение функционирования ТС обработки	Производится в текущий момент	1. Администратор ИБ принимает меры по немедленному удалению злоумышленника от СВТ.

информации злоумышленником		2. В случае если злоумышленник является пользователем системы, администратор ИБ блокирует доступ к ИСПДн. 3. В случае наличия повреждений администратор ИБ определяет ущерб, нанесенный ТС и информации. 4. Администратор ИБ производит восстановление работоспособности системы. 5. Производится служебная проверка и принимается соответствующее решение.
	Обнаружился случившийся факт	1. В случае наличия повреждений администратор ИБ определяет возможный круг лиц, причастных к нарушению, ущерб, нанесенный ТС и информации. 2. Администратор ИБ производит восстановление работоспособности системы. 3. Производится служебная проверка и принимается соответствующее решение.
Ошибки пользователей системмы при эксплуатации программных средств, ТС, средств и систем защиты информации	Ошибка повлекла утерю, повреждение защищаемой информации или привела к нарушению работоспособности ТС и ПО	1. Администратор ИБ проводит анализ и идентификацию причин инцидента. 2. Администратор ИБ определяет ущерб, нанесенный нештатной ситуацией. 3. Администратор ИБ проводит мероприятия по восстановлению работоспособности системы и информации. 4. Проводится проверка знаний работника виновного в инциденте, а в случае необходимости его обучение. 5. Администратор ИБ составляет акт об инциденте, в случае необходимости выносят предложение руководителю о применении дисциплинарной меры в отношении нарушителя.
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ		1. Администратор ИБ выявляют возможные причины проявления дестабилизирующих факторов. 2. В случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции отображенный в данной таблице. 3.Администратор ИБ восстанавливает работоспособность систем. 4. В случае потери данных Администратором ИБ по возможности проводится. восстановление их из резервных копий. 5. Администратором ИСПДн производится составление акта.
Сбои, отказы и аварии систем обеспечения ОИ		1. В случае если наблюдается продолжительное отключение электропитания. Администратором ИБ производится отключение СВТ

		до момента истечения резервов системы бесперебойного питания. 2. Ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения. 3. В случае потери защищаемых данных Администратором ИБ по возможности проводится восстановление их из резервных копий. 4. Ответственным за материально-техническое обеспечение производится составление акта.

Служебная проверка производится согласно Порядка проведения служебной проверки по фактам нарушения требований по обеспечению безопасности защищаемой информации.

Факт возникновения нештатной ситуации на ОИ подлежит обязательной регистрации работниками отдела по обеспечению безопасности деятельности в соответствующем журнале.

23. Ответственность за нарушение требований законодательства

Лица, виновные в нарушении норм законодательства в сфере защиты информации, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, предусмотренном законодательством РФ.

Приложение № 1

УТВЕРЖДАЮ
Директор
СПб ГБПОУ «УОР № 1»
_____ Ф.И.О.
м.п.
«___» _____ 20__ г.

«___» _____ 20__ г.

АКТ № _____
об уничтожении машинных носителей информации

Рабочая группа в составе:

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

провела отбор машинных носителей информации и установила, что в соответствии с требованиями с действующего законодательством Российской Федерации информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению, и составила настоящий акт о том, что произведено уничтожение машинных носителей информации.

№ п/п	Дата	Тип носителя	Учетный номер машинного носителя информации	Категория информации	Примечание

Всего машинных носителей информации: _____
(количество цифрами и прописью)

На указанных носителях информация уничтожена путем _____
_____.
(способ уничтожения защищаемой информации)

_____ /_____/

Председатель комиссии	*(Фамилия Имя Отчество)*	*(подпись)*
Члены комиссии	_____	/_____/
	(Фамилия Имя Отчество)	*(подпись)*
	_____	/_____/
	(Фамилия Имя Отчество)	*(подпись)*

_____

Приложение № 2

ФОРМА ЖУРНАЛА
учета машинных носителей информации

№ п/п	Наименование и тип машинного носителя	Учетный регистрационный (заводской) номер	Постановка на учет (дата, ФИО, подпись)	Место хранения, размещения, использования машинного носителя персональных данных	Лицо, ответственное за использование и хранение				Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
					Расписка в получении		Расписка в обратном приеме		
					ФИО	Дата, подпись	ФИО	Дата, подпись	

Приложение № 3

ФОРМА ЖУРНАЛА
учета нештатных ситуаций на объектах информатизации

№ п/п	Дата	Наименование и серийный номер технического средства	Краткое описание нештатной ситуации	Ф.И.О. и подпись администратора информационной безопасности	Примечание
1	2	3	4	5	6

Приложение № 4

УТВЕРЖДАЮ
Директор
СПб ГБПОУ «УОР № 1»
_____ Ф.И.О.
м.п.
«___» _____ 20__ г.

«___» _____ 20__ г.

АКТ № _____
о проведении внутреннего контроля

Комиссия в составе:

– председатель комиссии _____
(должность, Фамилия Имя Отчество)
– члены комиссии _____
(должность, Фамилия Имя Отчество)

_____
(должность, Фамилия Имя Отчество)

Привлечение независимых консультантов (аудитора): _____
_____

Проверяемый период: _____ 20__ года.
Фактические сроки проведения проверки: с ___ по ___ _____ 20__ года.

Комиссия провела внутренний контроль и (или) аудит соответствия обработки персональных данных текущему законодательству РФ, в том числе внутренним локальным-нормативным актами, в области обработки и защиты персональных данных.
В ходе проведения проверки было выявлено:
1._____
_____
_____
2._____
_____
_____
3._____
_____
_____

4._____
_____
_____
5._____
_____
_____
6._____
_____
_____

Для устранения нарушений необходимо:
1._____
_____
_____
2._____
_____
_____
3._____
_____
_____
4._____
_____
_____
5._____
_____
_____
6._____
_____
_____

Председатель комиссии _____ /_____/
(Фамилия Имя Отчество) *(подпись)*
Члены комиссии _____ /_____/
(Фамилия Имя Отчество) *(подпись)*
_____ /_____/
(Фамилия Имя Отчество) *(подпись)*

_____

Приложение № 5

УТВЕРЖДАЮ
Директор
СПб ГБПОУ «УОР № 1»
_____ Ф.И.О.
м.п.
«___» _____ 20__ г.

«___» _____ 20__ г.

АКТ № _____
установки средства защиты информации

Рабочая группа в составе:

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что были проведены работы по установке и настройке средств защиты информации (далее - СЗИ) на технические средства и системы, приведенные в таблице 1. Комплектация СЗИ соответствует приведенной в таблице 2.

Таблица 1.

Технические средства и системы, размещенные в помещении № _____,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), на жесткий диск которого установлено СЗИ*		
2	*Приводятся сведения о жестком диске, на*		

	который установлено СЗИ		

Таблица 2.

№ п/п	Наименование
1	2
1	*Сообщаются сведения о наименовании СЗИ*
1.1	*Сообщаются сведения о специальном защитном знаке, размещенном на установочном компакт-диске с программным обеспечением и эксплуатационной документацией*
1.2	*Сообщаются сведения о формуляре на СЗИ*
1.3	*Сообщаются сведения о сертификате соответствия на СЗИ*

Начальные установки параметров СЗИ выполнены в соответствии с требованиями нормативных документов по безопасности информации, а также в соответствии с руководствами по настройке программных продуктов, и представлены в приложении к настоящему акту.

По завершении установки и настройки СЗИ на корпусах технических средств и систем размещены пломбы (номерные наклейки) _____ .

По завершении установки и настройки СЗИ рабочей группой проведены проверки работоспособности основных функций СЗИ и реализованных механизмов защиты. Пользователь технических средств и систем с правилами работы СЗИ ознакомлен.

По результатам проверок, замечаний к работоспособности средств защиты информации и их настройке не выявлено.

Лицо, проводившее установку:

_____

(должность, подпись, расшифровка подписи)

Пользователь СЗИ:

_____

(должность, подпись, расшифровка подписи)

Приложение № 6

УТВЕРЖДАЮ
Директор
СПб ГБПОУ «УОР № 1»
_____ Ф.И.О.
м.п.
«___» _____ 20__ г.

«___» _____ 20__ г.

АКТ № ____
деинсталляции средства защиты информации

Рабочая группа в составе:

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании заявки/служебной записки _____
_____
(№, дата документа на инсталляцию СЗИ)

с технических средств и систем, приведенных в таблице 1, и находящихся в пользовании

(должность, фамилия, имя, отчество пользователя СЗИ)

произведена деинсталляция средства защиты информации (далее — СЗИ) _____
_____
(наименование, версия СЗИ)

следующим способом:[1]_____ .

Таблица 1.

Технические средства и системы, размещенные в помещении № _____,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер

[1] К способам уничтожения относятся переформатирование, удаление программного обеспечения СЗИ, физическое уничтожение носителей информации.

1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), с жесткого диска которого деинсталлировано СЗИ*		
2	*Приводятся сведения о жестком диске,* *с которого деинсталлировано СЗИ*		

Лицо, проводившее деинсталляцию:

_____

(должность, подпись, расшифровка подписи)

Пользователь СЗИ:

_____

(должность, подпись, расшифровка подписи)

_____

Приложение № 7

УТВЕРЖДАЮ
Директор
СПб ГБПОУ «УОР № 1»
_____ Ф.И.О.
м.п.
«___» _____ 20__ г.

«___» _____ 20__ г.

АКТ № _____
о проведении служебной проверки по факту нарушения требований по обеспечению безопасности защищаемой информации

Комиссия в составе:

– председатель комиссии _____
(должность, Фамилия Имя Отчество)

– члены комиссии _____
(должность, Фамилия Имя Отчество)

_____
(должность, Фамилия Имя Отчество)

Привлечение независимых консультантов (аудитора): _____
_____

Проверяемый период: _____ 20__ года.
Фактические сроки проведения проверки: с ___ по ___ _____ 20__ года.
Основанием для проведения проверки послужило: _____
_____
_____

В ходе проведения проверки было выявлено:
1. _____
_____
2. _____
_____
3. _____
_____
4. _____
_____
5. _____
_____
6. _____
_____
7. _____
_____

Для устранения нарушений необходимо:

1. _____
_____
2. _____
_____
3. _____
_____
4. _____
_____
5. _____
_____
6. _____
_____
7. _____
_____

Председатель комиссии _____ /_____/
(Фамилия Имя Отчество) *(подпись)*

Члены комиссии _____ /_____/
(Фамилия Имя Отчество) *(подпись)*

_____ /_____/
(Фамилия Имя Отчество) *(подпись)*

Приложение № 8

УТВЕРЖДАЮ
Директор
СПб ГБПОУ «УОР № 1»
_____ Ф.И.О.
м.п.
«___» _____ 20__ г.

АКТ № ____

«___» _____ 20 __ г.

об уничтожении персональных данных

Настоящий акт составлен комиссией по уничтожению персональных данных, созданной приказом Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Училище олимпийского резерва № 1» от _____ № ___, в составе:

Заместитель председателя комиссии	Заместитель директора по безопасности	Ф.И.О.
Секретарь комиссии:	Специалист по защите информации отдела по обеспечению безопасности деятельности	Ф.И.О.
Члены комиссии:	Начальник отдела по обеспечению безопасности деятельности	Ф.И.О.
	Начальник отдела кадров и правовой работы	Ф.И.О.
	Начальник отдела, который выносит документы на рассмотрение комиссии	Ф.И.О.
	Юрисконсультант отдела кадров и правовой работы	Ф.И.О.

Акт составлен о том, что в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Училище олимпийского резерва № 1, ОГРН 1027802519370, ИНН 7804029740, юридический адрес: 195220, г. Санкт-Петербург, ул. Гжатская, д. 4,

уничтожены персональные данные, представленные: Ф.И.О. _____.
Категории уничтоженных ПДн: _____.
С помощью физического уничтожения, путем помещения в шредер.
Наименование носителя (кол-во листов): _____.
Уничтожено на основании: _____.
Указанные данные были уничтожены в присутствии членов комиссии.

Заместитель председателя комиссии:

Заместитель директора по безопасности	_____	Ф.И.О.

Секретаря комиссии:

Специалист по защите информации отдела по обеспечению безопасности деятельности	_____	Ф.И.О.

Члены комиссии:

Начальник отдела по обеспечению безопасности деятельности	_____	Ф.И.О.
Начальник отдела кадров и правовой работы	_____	Ф.И.О.
Начальник отдела, который выносит документы на рассмотрение комиссии	_____	Ф.И.О.
Юрисконсультант отдела кадров и правовой работы	_____	Ф.И.О.