

<p>Принято На педагогическом Совете 29 августа 2024 года Протокол №1</p>	<p>Утверждено Приказом МАОУ СОШ с углубленным изучением отдельных предметов № 50 От 05 сентября 2024 года Директор  Ю. В. Дорофеева</p> 
--	---

ПОЛОЖЕНИЕ
по организации и проведению работ
по обеспечению безопасности
защищаемой информации при ее обработке
в МАОУ СОШ № 50

Содержание

Список сокращений и обозначений.....	5
1. Термины и определения	6
2. Нормативно-методическое обеспечение	8
3. Общие положения	10
4. Пользователь ИС	11
4.1. Обязанности пользователя ИС.....	11
4.2. Ответственность пользователя ИС	12
4.3. Права пользователя ИС.....	13
5. Первичный инструктаж лица, допущенного к работе с защищаемой информацией.....	14
6. Обработка персональных данных без использования средств автоматизации 15	15
6.1. Организация обработки персональных данных, осуществляемой без использования средств автоматизации	15
6.2. Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации	17
7. Организация режима обеспечения безопасности помещений, в которых осуществляется обработка защищаемой информации	18
7.1. Общие сведения.....	18
7.2. Требования к помещениям, предназначенным для размещения архивов	19
8. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации	21
8.1. Внешний контроль над соблюдением требований по обработке и обеспечению защищаемой информации	21
8.2. Внутренний контроль за обеспечением уровня защищенности информации	21
8.2.1. Порядок внутреннего контроля за обеспечением уровня защищенности информации	21
8.2.2. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».....	23
8.2.3. Соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»	23
9. Порядок проведения служебной проверки по фактам нарушения требований по обеспечению безопасности защищаемой информации.....	25
9.1. Классификация нарушений требований по обеспечению безопасности защищаемой информации	25
9.2. Перечень нарушений требований по обеспечению безопасности защищаемой информации	25
9.3. Назначение и проведение служебной проверки.....	27
9.4. Оформление результатов работы комиссии	28
10. Порядок приостановления обработки персональных данных.....	29
11. Обезличивание персональных данных	30
11.1. Условия обезличивания персональных данных	30
11.2. Методы обезличивания персональных данных.....	30

11.3. Процедура обезличивания.....	30
11.4. Организация обработки ПДн и обезличенных данных	30
11.5. Рекомендации по выбору методов обезличивания в соответствии с классом задач обработки.....	31
12. Уничтожение защищаемой информации.....	34
12.1. Условия уничтожения защищаемой информации	34
12.2. Порядок уничтожения защищаемой информации	34
12.3. Способы уничтожения защищаемой информации	34
13. Порядок управления доступом субъектов доступа к объектам доступа в информационной системе.....	36
14. Организация парольной защиты в ИС	37
14.1. Общие положения	37
14.2. Порядок организации парольной защиты.....	37
14.3. Порядок применения парольной защиты.....	38
15. Организация идентификации и аутентификации пользователей ИС	39
15.1. Управление идентификаторами	39
15.2. Управление аутентификационной информацией.....	39
16. Организация антивирусной защиты в ИС	41
16.1. Общие положения	41
16.2. Порядок организации антивирусной защиты.....	41
17. Организация учета машинных носителей защищаемой информации.....	43
17.1. Порядок учета машинных носителей защищаемой информации	43
17.2. Порядок хранения машинных носителей защищаемой информации.....	43
17.3. Порядок эксплуатации машинных носителей защищаемой информации	44
18. Организация резервирования и восстановления информации в ИС	45
18.1. Общие положения	45
18.2. Информация, подлежащая резервному копированию	45
18.3. Порядок резервирования и хранения резервных копий	45
18.4. Порядок восстановления работоспособности информационной системы.....	46
19. Порядок работы с электронными журналами протоколирования и анализа (аудита) значимых событий (регистрация событий безопасности)	47
20. Порядок обращения со средствами защиты информации	49
20.1. Учет средств защиты информации	49
20.2. Распространение средств защиты информации	49
20.3. Получение средств защиты информации.....	50
20.4. Уничтожение средств защиты информации.....	50
20.5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства защиты информации	51
20.6. Ответственность за нарушение требований эксплуатации средств защиты.....	51
21. Порядок обеспечения информационной безопасности ИС при модернизации (обновлении) аппаратных и программных компонентов.....	52
22. Управление конфигурацией информационной системы и ее системы защиты.....	53
23. Анализ защищенности информации при ее обработке в ИС	55
24. Выявление инцидентов безопасности и реагирование на них	56
24.1. Общие сведения.....	56
24.2. Обнаружение, идентификация и регистрация инцидентов безопасности.....	57
24.3. Планирование и принятие мер по предотвращению инцидентов безопасности	58
24.4. Реагирование на инциденты, повлекшие неправомерную передачу (предоставление, распространение, доступ) персональных данных.....	58

25. Правила и процедуры информирования и обучения персонала	60
25.1. Цели и задачи обучения вопросам информационной безопасности	60
25.2. Виды обучения и проверки знаний	60
25.3. Организация обучения и проверки знаний	61
26. Правила и процедуры планирования мероприятий по обеспечению безопасности	63
26.1. Основные цели планирования	63
26.2. Планирование контрольных мероприятий	63
26.3. Оформление результатов контрольных мероприятий	64
27. Ответственность за нарушение требований законодательства	65
Приложение № 1	66
Приложение № 2 –А	67
Приложение № 3	0
Приложение № 4	1
Приложение № 5	2
Приложение № 6	3
Приложение № 7	4
Приложение № 8	5
Приложение № 9	6
Приложение № 10	7
Приложение № 11	8
Приложение № 12	9
Приложение № 13	10
Приложение № 14	11
Приложение № 15	13
Приложение № 16	14
Приложение № 17	16
Приложение № 18	17
Приложение № 19	18
Приложение № 20	19
Приложение № 21	20

Список сокращений и обозначений

АРМ	Автоматизированное рабочее место
БД	База данных
ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
ТС	Техническое средство

1. Термины и определения

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.

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 – ПДн) – 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.

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

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

Объект доступа (в автоматизированной ИС) – единица ресурса автоматизированной ИС, доступ к которой регламентируется правилами разграничения доступа.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с 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 ИС) – 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, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

2. Нормативно-методическое обеспечение

Настоящее Положение по организации и проведению работ по обеспечению безопасности защищаемой информации при ее обработке в МАОУ СОШ № 50 (далее – Положение) разработано на основании:

[1] – Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] – Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

[3] – постановления Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

[4] постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[5] приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[6] приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[7] приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

[8] методических рекомендаций по применению приказа Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденные 13.12.2013 г. руководителем Роскомнадзора;

[9] приказа Роскомнадзора от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;

[10] приказа Роскомнадзора от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

[11] приказа Роскомнадзора от 14.11.2022 г. № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»;

[12] ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (введен в действие 01.01.2022 г.);

[13] ГОСТ Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (введен в действие 01.01.2006 г.);

[14] ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию» (введен в действие 01.02.2008 г.);

[15] ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (введен в действие 01.02.2008 г.).

3. Общие положения

Настоящее Положение определяет порядок организации и проведения работ по обеспечению безопасности персональных данных и информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (далее – защищаемая информация) при ее обработке в МАОУ СОШ № 50 (далее – Оператор).

Положение разработано с целью:

- организации и координации работ по обеспечению безопасности защищаемой информации в государственных информационных системах;
- регламентации порядка проведения работ по обеспечению безопасности защищаемой информации, обрабатываемой в информационных системах и информационных системах персональных данных МАОУ СОШ № 50 (далее – ИС);
- контроля состояния безопасности защищаемой информации, обрабатываемой в ИС;
- 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. Пользователь ИС

4.1. Обязанности пользователя ИС

Пользователем ИС является сотрудник, который в силу своих должностных обязанностей осуществляет обработку защищаемой информации с использованием средств автоматизации и имеет доступ к информационным ресурсам, аппаратным средствам, ПО и средствам защиты информации.

Пользователь ИС несет персональную ответственность за свои действия.

Пользователь ИС в своей работе руководствуется нормативными правовыми актами в сфере персональных данных и локальными актами Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке.

Пользователь ИС обязан:

- соблюдать требования нормативных правовых актов в сфере защиты информации и локальных актов Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при их обработке в ИС;

- выполнять на АРМ в отношении защищаемой информации только те процедуры, которые определены для него в локальных актах Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке в ИС;

- в случае временного отсутствия на рабочем месте для предотвращения доступа к информации, находящейся на АРМ, минуя ввод пароля, пользователь ИС во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню или выключить АРМ. По окончании рабочего дня пользователь ИС обязан выключить АРМ;

- знать и соблюдать установленные требования по обработке и обеспечению безопасности ПДн;

- соблюдать требования антивирусной защиты в ИС;

- соблюдать требования парольной защиты в ИС;

- соблюдать правила при работе в сетях общего доступа и (или) международного обмена;

- контролировать доступ посторонних лиц в помещения, в которых расположены компоненты ИС;

- контролировать наличие и целостность пломб на корпусах технических средств в составе ИС.

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

Работа в сетях связи общего пользования и (или) сетях международного информационного обмена (далее – Сеть) на элементах ИС должна проводиться при служебной необходимости.

При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусное средство, межсетевой экран и другие);

- скачивать из Сети ПО и другие файлы;
- посещение сайтов, непосредственно не связанных с исполнением служебных обязанностей;
- нецелевое использование подключения к Сети.

Обо всех выявленных нарушениях требований по обработке и обеспечению безопасности защищаемой информации пользователь ИС должен незамедлительно сообщать администратору информационной безопасности либо руководству.

Для получения консультаций по вопросам работы и настройке элементов ИС пользователь ИС должен обращаться к администратору информационной безопасности.

Пользователь ИС обязан принимать меры по реагированию в случае возникновения нештатных либо аварийных ситуаций, с целью ликвидации их последствий в рамках, возложенных на него функций.

Пользователю ИС запрещается:

- разглашать защищаемую информацию третьим лицам;
- сообщать, передавать посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС;
- сообщать (или передавать) посторонним лицам сведения о системе защиты ИС;
- обрабатывать защищаемую информацию в условиях, позволяющих осуществлять просмотр защищаемой информации лицами, не имеющими к ним права доступа, а также при несоблюдении требований по обеспечению безопасности информации;
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временное блокирование ОС нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню);
- самостоятельно вносить изменения в конфигурацию ПО и ТС ИС, изменять установленный алгоритм функционирования технических и программных средств;
- записывать и хранить защищаемую информацию, на неучтенных установленном порядке машинных носителях информации;
- использовать АРМ и другие ресурсы ИС в неслужебных целях;
- подключать к АРМ личные машинные носители информации и мобильные устройства;
- отключать (блокировать) СЗИ;
- привлекать посторонних лиц для ремонта или настройки АРМ без согласования с администратором информационной безопасности.

4.2. Ответственность пользователя ИС

Пользователь ИС несет ответственность за:

- неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящим Положением в пределах, определенных трудовым законодательством РФ; совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определенных административным, уголовным и гражданским законодательством РФ;

- невыполнение или ненадлежащее выполнение поручений директора;
- эксплуатацию ИС;
- сохранность защищаемой информации;
- соблюдение требований нормативных правовых актов в сфере защиты информации и локальных актов Оператора, определяющих порядок организации и проведения работ, направленных на обеспечение безопасности защищаемой информации при ее обработке в ИС;
 - сохранность и работоспособное состояние ТС, ПО, средств защиты, входящих в состав ИС;
 - выполнение обязанностей, предусмотренных настоящим Положением.

4.3. Права пользователя ИС

Пользователь ИС имеет права:

- осуществлять обработку защищаемой информации в пределах установленных полномочий;
- обращаться к администратору информационной безопасности за оказанием технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, ТС ИС, а также с СЗИ.

5. Первичный инструктаж лица, допущенного к работе с защищаемой информацией

Первичный инструктаж лица, допущенного к работе с защищаемой информацией (далее – лицо), проводит администратор информационной безопасности после утверждения директором документа о наделении лица правом доступа к защищаемой информации до непосредственного доступа этого лица к защищаемой информации.

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

Лицо должно быть ознакомлено с нормативными правовыми актами РФ в сфере защиты информации.

Лицо должно быть ознакомлено с локальными актами Оператора, регламентирующими вопросы защиты информации.

Лицо, являющееся пользователем ИС, должно иметь доступ только к тем функциям ИС, которые необходимы для выполнения им его должностных обязанностей.

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

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

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

- о проведении разбирательств по фактам совершения действий, связанных с доступом к защищаемой информации 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 администратором информационной безопасности в соответствующем журнале учета пользователей, имеющих право доступа к информационным системам, форма которого приведена в Приложении № 1 к настоящему Положению.

6. Обработка персональных данных без использования средств автоматизации

6.1. Организация обработки персональных данных, осуществляемой без использования средств автоматизации

Порядок обработки персональных данных, осуществляемой без использования средств автоматизации осуществляется в соответствии с [3].

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях, обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, а также настоящим порядком.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, полное наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку ПДн;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Оператора, или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Оператора, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится Оператор, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

– копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

– ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Оператора.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению отдельной обработки ПДн, в частности:

– при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

– при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

6.2. Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключаящие несанкционированный к ним доступ.

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 Оператора, где осуществляется обработка защищаемой информации, разрешается только в присутствии лиц, имеющих право доступа к защищаемой информации, обрабатываемой в соответствующем помещении.

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

Защищаемая информация на бумажных носителях и машинные носители защищаемой информации (диски, флеш-карты) должны храниться в недоступном для посторонних лиц месте: в шкафах, оборудованных замками.

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

Вскрытие и закрытие помещений, в которых ведется обработка защищаемой информации, производится сотрудниками Оператора, имеющими право доступа к защищаемой информации, обрабатываемой в соответствующем помещении.

Перед закрытием помещений, в которых осуществляется обработка защищаемой информации, по окончании служебного дня сотрудники, имеющие право доступа к защищаемой информации, обрабатываемой в соответствующем помещении, обязаны:

- убрать бумажные носители защищаемой информации и машинные носители защищаемой информации (диски, флеш-карты) в запираемые шкафы, запереть шкафы на замок;
- отключить ТС (кроме постоянно действующего оборудования) и электроприборы от сети, выключить освещение;
- закрыть окна, двери.

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

- не вскрывая помещение, в котором осуществляется обработка защищаемой информации, сообщить об этом директору;
- в присутствии не менее двух сотрудников, включая директора, вскрыть помещение и осмотреть его;

– составить акт о выявленных нарушениях и передать установленным порядком директору.

При работе с защищаемой информации двери помещений должны быть всегда закрыты.

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 к защищаемой информации, обрабатываемой в соответствующем помещении, после принятия мер, исключающих визуальный просмотр документов, содержащих защищаемую информацию, и экранов мониторов.

Корпус ТС, с которым осуществляется штатное функционирование ИС, должен быть оборудован средствами контроля их вскрытия (опечатаны, опломбированы), место опечатывания (опломбирования) должно быть визуально контролируемым. Внутренняя планировка и расположение рабочих мест в помещениях, где осуществляется обработка защищаемой информации, должны исключать визуальный просмотр обрабатываемой защищаемой информации для сотрудников, не осуществляющих обработку такой информации. Окна помещений, в которых осуществляется обработка защищаемой информации, должны быть оборудованы шторами (жалюзи).

В случае, когда помещения, в которых осуществляется обработка защищаемой информации, располагаются на первых и последних этажах здания, их окна должны быть оснащены прочными решетками или жалюзи.

На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, в которых предусматривается порядок вызова сотрудников, вскрытие помещений, где осуществляется обработка защищаемой информации, очередность и порядок эвакуации документов, материалов и изделий, содержащих защищаемую информацию, а также порядок дальнейшего их хранения.

Ответственность за соблюдение порядка доступа в помещения, в которых осуществляется обработка защищаемой информации, возлагается на руководителей структурных подразделений, осуществляющих обработку защищаемой информации, а также на руководителя Оператора.

7.2. Требования к помещениям, предназначенным для размещения архивов

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

- помещение должно располагаться в контролируемой зоне;
- двери помещения должны иметь надежные запоры, приспособления для опечатывания, либо должны быть оснащены контроллерами, включенными в систему контроля ограничения доступа;

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

– должны быть задействованы все меры, исключая неконтролируемое пребывание в помещении любых лиц, включая сотрудников, 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 пульта 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.

Сотрудник, осуществляющий хранение архивов и/или резервных копий ИС, должен иметь печать для опечатывания дверей и сейфа или металлического хранилища.

8. Контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации

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

- внешний контроль и надзор за соблюдением требований по обработке и обеспечению безопасности защищаемой информации;
- внутренний контроль за обеспечением уровня защищенности информации (в т.ч. внутренний контроль соответствия обработки защищаемой информации требованиям к обеспечению безопасности защищаемой информации) (далее – внутренний контроль за обеспечением уровня защищенности информации).

Внутренний контроль за обеспечением уровня защищенности информации осуществляется Оператором и состоит из:

- контроля и надзора за исполнением требований по обработке и обеспечению безопасности защищаемой информации с учетом ее уровня защищенности;
- оценки соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер.

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

Внешний контроль и надзор за выполнением требований законодательства в области защиты информации осуществляется:

- Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в пределах своих полномочий;
- Федеральной службой безопасности РФ в пределах своих полномочий.
- Федеральной службой по техническому и экспортному контролю в пределах своих полномочий.

8.2. Внутренний контроль за обеспечением уровня защищенности информации

8.2.1. Порядок внутреннего контроля за обеспечением уровня защищенности информации

Оператор при обработке защищаемой информации обязан принимать необходимые правовые, организационные и технические меры для обеспечения безопасности защищаемой информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении защищаемой информации.

Внутренний контроль за обеспечением уровня защищенности информации – это комплекс мероприятий, осуществляемых в целях:

- соблюдения условий и принципов обработки защищаемой информации;
- соблюдения требований по обработке и обеспечению безопасности защищаемой информации;
- предупреждения и пресечения возможности получения посторонними лицами защищаемой информации;
- выявления и предотвращения утечки защищаемой информации по техническим каналам;
- исключения или затруднения несанкционированного доступа к защищаемой информации;
- хищения ТС, входящих в состав ИС, и машинных носителей защищаемой информации;
- предотвращения программно-математических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности ИС.

Основными задачами внутреннего контроля за обеспечением уровня защищенности информации являются:

- проверка соответствия локальных актов в области защищаемой информации действующему законодательству РФ;
- соблюдение прав субъектов ПДн, чьи ПДн обрабатываются Оператором;
- наличие необходимых согласий субъектов ПДн, чьи ПДн обрабатываются Оператором;
- проверка актуальности содержания локальных актов в области обеспечения безопасности защищаемой информации;
- проверка соблюдения требований нормативных правовых актов, методических документов в сфере обеспечения безопасности защищаемой информации при подготовке организационно-распорядительной документации;
- проверка организации и выполнения мероприятий по обеспечению безопасности защищаемой информации при ее обработке как с использованием средств автоматизации, так и без использования средств автоматизации;
- проверка работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- наличие эксплуатационной документации на технические и программные средства защиты ИС;
- оценка знаний и качества выполнения сотрудниками своих функциональных обязанностей в части защиты информации;
- оперативное принятие мер по пресечению нарушений требований по обеспечению безопасности информации при ее обработке в ИС.

Внутренний контроль за обеспечением уровня защищенности информации осуществляется ответственным за обеспечение уровня защищенности информации в ИС 1 (Один) раз в полгода. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, администратор информационной безопасности докладывает руководству и производит отметку в журнале учета проведения контроля за обеспечением уровня защищенности информации, приведенном в Приложении № 13.

8.2.2. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

Оценкой вреда, который может быть причинен субъектам ПДн в случае нарушения [2] является определение юридических последствий в отношении субъекта ПДн, которые могут возникнуть в случае нарушения [2].

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

При обработке ПДн должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта ПДн, которые могут возникнуть в случае нарушения [2].

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения [2], оформляется документально.

8.2.3. Соотношение вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»

Во время осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн производится оценка соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения [2] и применяемых мер, направленных на выполнение обязанностей, предусмотренных [2].

При оценке соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения [2], для ИС производится экспертное сравнение заявленной Оператором в своих локальных актах оценки вреда, который может быть причинен субъектам ПДн в случае нарушения [2] и применяемых мер, направленных на выполнение обязанностей, предусмотренных [2], и изложенных в настоящем Положении.

По итогам сравнений принимается решение о достаточности применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и возможности или необходимости принятия дополнительных мер или изменения установленного порядка организации и проведения работ по обеспечению безопасности ПДн при их обработке.

Оценка соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований [2] и применяемых мер, направленных на выполнение

обязанностей, предусмотренных [2], оформляется в виде отдельного документа, подписывается ответственным лицом.

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 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 ИС, а именно:

- успешный подбор административного пароля;
- несанкционированная реконфигурация параметров ИС;
- утрата или кража резервной копии базы, содержащей защищаемую информацию;
- необоснованная передача информационных массивов ИС;
- организация утечки сведений по техническим каналам;
- умышленное нарушение работоспособности ИС;
- НСД к защищаемой информации;
- несанкционированное внесение изменений в ИС;
- умышленное заражение АРМ и серверов, входящих в состав ИС, вирусами;
- проведение работ с ИС, повлекшее 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 от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	
ст. 17	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»	
ст. 24	Ответственность за нарушение требований настоящего Федерального закона

1	2
Кодекс Российской Федерации 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 Российской Федерации	
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 Российской Федерации	
ст. 90	Ответственность за нарушение норм, регулирующих обработку и защиту ПДн сотрудника

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 ИС, а именно:

- ошибка при входе в ИС (набор не назначенного пароля, более 3 (Трех) раз подряд, периодически);
- оставление АРМ включенным (незаблокированным) во время отсутствия на рабочем месте;
- перезагрузка АРМ при сбоях в работе, в т.ч. аварийная (неоднократная) перезагрузка путем нажатия кнопки RESET;
- утрата учтенного машинного носителя защищаемой 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) программного обеспечения (далее – ПО) в ИС;
- несанкционированное изменение конфигурации ПО ИС;

- попытка получения прав администратора на АРМ (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 АРМ компьютерными вирусами;
- несанкционированное использование сканирующего ПО;
- несанкционированное использование анализаторов протоколов (снифферов);
- несанкционированный просмотр, вывод на печать и т.п. защищаемой информации.

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

- ошибка при входе в ИС (набор неправильного пароля, сетевого имени более 3 (Трех) раз подряд, не периодическая);
- периодическая попытка неудачного доступа к защищаемой информации ИС;
- перевод времени на АРМ;
- однократная перезагрузка АРМ при сбоях в работе АРМ, в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;
- нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

9.3. Назначение и проведение служебной проверки

Служебная проверка назначается по нарушениям I и II категорий.

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

Служебная проверка проводится комиссией, состав которой утверждает директор _____.

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 сотрудника Оператора.

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

За назначение процедуры служебной проверки ответственность несет руководитель Оператора.

9.4. Оформление результатов работы комиссии

Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения на имя директора 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, 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 защищаемой информации или к снижению уровня защищенности ПДн;
- 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 персональных данных

При обнаружении нарушений I категории обработка ПДн незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

Принятие решения о приостановлении обработки ПДн принимается руководителем Оператора.

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

11. Обезличивание персональных данных

11.1. Условия обезличивания персональных данных

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 [8].

11.2. Методы обезличивания персональных данных

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 персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);
- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств);
- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

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 в информационную систему.

Оператор вправе обрабатывать в информационной системе 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 Оператором. 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 Оператора 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 Оператору 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

Класс задач	Задачи обработки	Метод обезличивания
1	2	3
Статистическая обработка и статистические исследования ПДн	– осуществление выборки по заявленным параметрам; – проведение исследований по заданным параметрам субъектов.	– метод перемешивания; – метод декомпозиции; – метод изменения состава или семантики.
Сбор и хранение ПДн	– 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 ПДн	– внесение изменений в существующие записи о субъектах на основе обращений субъектов, решений судов и других уполномоченных органов;	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.

1	2	3
	– внесение изменений в существующие записи о субъектах на основе исследований, выполнения органом своих функций или требований законодательства РФ.	
Интеграция данных различных операторов	– поиск информации о субъектах; – передача данных смежным органам.	– метод перемешивания; – метод декомпозиции; – метод введения идентификаторов.
Ведение учета субъектов ПДн	– 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

12.1. Условия уничтожения защищаемой информации

Уничтожение защищаемой информации должно быть проведено:

– по достижении целей обработки защищаемой информации или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

– 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.

В случае обращения субъекта ПДн к МАОУ СОШ № 50 с требованием о прекращении обработки ПДн. МАОУ СОШ № 50 обязано в срок, не превышающий десяти рабочих дней с даты получения МАОУ СОШ № 50 соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 [2]. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления МАОУ СОШ № 50 в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В случае отсутствия возможности уничтожения ПДн, в течение указанного срока, указанного в частях 3-5.1 ст. 20 [2] МАОУ СОШ № 50 осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению МАОУ СОШ № 50) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

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;

– уничтожить защищаемую информации подходящим способом, указанным в соответствующем требовании или распорядительном документе;

– 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 машинного носителя информации.

Для физического уничтожения бумажного носителя с защищаемой информацией используются два вида уничтожения – уничтожение через shredding (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 ее наличия в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено действующим законодательством РФ.

Если защищаемая информация хранится 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 защищаемой информации (за исключением персональных данных) составляется Акт уничтожения защищаемой информации либо Акт уничтожения машинных носителей информации, формы которых приведены в Приложении № 2-А и в Приложении № 3 к настоящему Положению.

Если обработка персональных данных осуществляется без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных (Приложение № 2-Б).

Если обработка персональных данных осуществляется с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных (Приложение № 2-Б) и выгрузка из журнала регистрации событий в информационной системе персональных данных.

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 в информационной системе

Предоставление доступа пользователю к ИС (или изменение прав доступа) осуществляется на основании Перечня лиц, имеющих право доступа к защищаемой информации, обрабатываемой в ИС, утвержденного директором.

С целью организации учета лиц, имеющих право доступа к защищаемой информации, обрабатываемой в ИС, ведется журнал учета пользователей, имеющих право доступа к информационным системам, форма которого приведена в Приложении № 1 к настоящему Положению.

Назначение прав доступа пользователей к защищаемой информации в ИС осуществляется администратором информационной безопасности в соответствии с заявками на предоставление пользователю ИС прав доступа к ИС (ресурсу ИС) от руководителя структурного подразделения, оформляемыми по форме, приведенной в Приложении № 4 к настоящему Положению. При этом в журнале учета пользователей, имеющих право доступа к информационным системам, производится соответствующая запись.

Все факты несанкционированной организации доступа и регистрации в ИС, а также их последствия классифицируются в соответствии с Перечнем нарушений требований по обеспечению безопасности защищаемой информации.

Контроль за деятельностью пользователей ИС ведётся администратором информационной безопасности.

Наличие у сотрудника избыточных, неконтролируемых прав доступа является нарушением требований по обеспечению безопасности защищаемой информации.

Основанием для прекращения права доступа пользователя к ИС может служить его исключение из утвержденного директором Перечня лиц, имеющих право доступа к защищаемой информации, обрабатываемой в ИС, или его увольнение.

14. Организация парольной защиты в ИС

14.1. Общие положения

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

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

Организационное и техническое обеспечение процессов выдачи, использования, смены и прекращения действия паролей во всех подсистемах ИС 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 АРМ, входящей в состав ИС;
- настройки ОС;
- настройки сетевого оборудования;
- настройки СЗИ;
- ПО, предназначенное для обработки защищаемой информации;
- ресурсы АРМ и информационные ресурсы, содержащие защищаемую информацию.

Личные пароли доступа пользователей ИС генерируются и распределяются централизованно или выдаются администратором информационной безопасности, или выбираются пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 (Восьми) буквенно-цифровых символов;
- 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 АРМ, общепринятые сокращения (например, ЭВМ, ЛВС, USER, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе ИС;
- 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;
- в числе символов пароля обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, а также цифры и символы;
- не допускается использование ранее использованных пароли.

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 АРМ, 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

Полная плановая смена паролей проводится администратором информационной безопасности один раз в 3 (Три) месяца.

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

Для предотвращения доступа к информации, находящейся в АРМ, минуя ввод пароля, пользователь ИС во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню или выключить АРМ.

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

Факт выдачи пароля пользователю ИС фиксируется в журнале учета выдачи паролей для доступа к информационным системам, форма которого приведена в Приложении № 5 к настоящему Положению.

Ответственность за организацию парольной защиты возлагается на администратора информационной безопасности.

Ответственность за соблюдение требований парольной защиты возлагается на администратора информационной безопасности и пользователей ИС.

Нарушения организации и порядка применения парольной защиты классифицируются в соответствии с Перечнем нарушений требований по обеспечению безопасности защищаемой информации.

При выявлении нарушений I и II категории проводится служебная проверка в соответствии с Порядком проведения служебной проверки по фактам нарушения требований по обеспечению защищаемой информации.

15. Организация идентификации и аутентификации пользователей ИС

Управление атрибутами доступа пользователей ИС (идентификаторы и пароли) осуществляется администратором информационной безопасности.

Запрещены действия пользователей до прохождения ими процедур идентификации и аутентификации в ИС.

15.1. Управление идентификаторами

Процессы формирования, присвоения, смены и прекращения действия идентификаторов выполняются администратором информационной безопасности.

При добавлении нового пользователя ИС (установленным порядком) администратор информационной безопасности должен зарегистрировать для него персональный идентификатор.

Идентификатор подлежит блокировке в следующих случаях:

- при неиспользовании идентификатора более трех месяцев;
- при увольнении владельца идентификатора – с целью предотвращения его повторного использования – немедленно после окончания последнего сеанса работы данного пользователя с системой.

Удалению подлежат идентификаторы, заблокированные более трех лет.

15.2. Управление аутентификационной информацией

Защите паролем (при наличии такой технической возможности) подлежит доступ к следующим ресурсам:

- базовым системам ввода-вывода компьютеров;
- настройкам сетевого оборудования;
- настройкам операционных систем;
- настройкам средств защиты информации (в том числе средств антивирусной защиты);
- запуску специализированного программного обеспечения, предназначенного для обработки защищаемой информации (в том числе персональных данных);
- ресурсам информационных систем, содержащих защищаемую информацию.

Объекты парольной защиты необходимо настраивать таким образом, чтобы:

- исключить возможность просмотра ранее вводимых паролей;
- блокировать доступ пользователей к ИС после неоднократной ошибки при вводе пароля (правом снятия блокировки обладает только администратор информационной безопасности);
- автоматически блокировать сеанс доступа пользователя ИС после его бездействия (неактивности) в течение установленного времени;
- исключить ознакомление посторонних лиц с аутентификационной информацией в процессе ее ввода (защита обратной связи).

Запрещается пользоваться аутентификационной информацией, заданной производителем технического средства (программного обеспечения).

Личные пароли доступа пользователей ИС генерируются и выдаются администратором информационной безопасности с учетом следующих требований:

- длина пароля должна быть не менее 12 (Двенадцати) буквенно-цифровых символов;

- 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 АРМ, общепринятые сокращения (например, ЭВМ, ЛВС, USER, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе ИС;

- 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.);

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

- не допускается использование ранее использованных пароли.

Факт выдачи пароля пользователю ИС фиксируется в журнале учета выдачи паролей для доступа к информационным системам, форма которого приведена в Приложении № 5 к настоящему Положению.

Разрешается использовать специализированное программное обеспечение для формирования паролей.

Полная плановая смена паролей проводится один раз в 3 (Три) месяца.

Внеплановая смена пароля пользователя ИС должна производиться в случае прекращения полномочий пользователя после завершения последнего сеанса работы данного пользователя с системой.

В случае прекращения полномочий администратора информационной безопасности производится внеплановая полная смена всех паролей, к которым он имел доступ.

В случае компрометации личного пароля должны быть немедленно предприняты вышеуказанные меры в зависимости от полномочий владельца скомпрометированного пароля.

Для предотвращения доступа к информации, находящейся в АРМ, минуя ввод пароля, пользователь ИС во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню или выключить АРМ.

При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах (например, на мониторе АРМ, на обратной стороне клавиатуры);

- хранить пароли в записанном виде на отдельных листах бумаги;

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

16. Организация антивирусной защиты в ИС

16.1. Общие положения

Целью антивирусной защиты ИС является предотвращение и нейтрализация негативных воздействий вредоносного ПО на информационные ресурсы, содержащие защищаемую информацию, и ПО, предназначенного для обработки защищаемой информации.

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

К использованию в ИС допускаются только лицензионные и сертифицированные ФСТЭК России по требованиям безопасности информации средства защиты от вредоносного ПО.

Установка и начальная настройка средств защиты от вредоносного ПО в ИС может осуществляться администратором информационной безопасности, а также представителями организации-лицензиата ФСТЭК России.

Администратор информационной безопасности должен организовывать осуществление периодического обновления сигнатур средств защиты от вредоносного ПО и контроль их работоспособности не реже 1 (Одного) раза в неделю.

Пользователи ИС обязаны руководствоваться в работе Порядком организации антивирусной защиты.

16.2. Порядок организации антивирусной защиты

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), защищаемая информация, содержащиеся 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. Периодические проверки электронных архивов проводятся администратором информационной безопасности не реже 1 (Одного) раза в месяц.

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

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

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

- приостановить работу АРМ;
- немедленно поставить в известность о факте обнаружения вредоносного ПО администратора информационной безопасности, а также других пользователей ИС, использующих зараженные файлы в работе;
- совместно с владельцем зараженных вредоносным ПО файлов провести анализ возможности их дальнейшего использования;
- провести «лечение» или удаление зараженных файлов.

Периодически, но не реже 1 (Одного) раза в неделю, администратором информационной безопасности должна проводиться антивирусная проверка всех жестких дисков АРМ пользователей ИС.

Антивирусные проверки подлежат регистрации в журнале учета антивирусных проверок информационных систем, форма которого приведена в Приложении № 6 к настоящему Положению.

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

17. Организация учета машинных носителей защищаемой информации

17.1. Порядок учета машинных носителей защищаемой информации

Регистрации и учету подлежат все машинные носители информации, содержащие защищаемую информацию, а именно:

- жесткие диски, находящиеся в системных блоках серверов;
- жесткие диски, находящиеся во внешних RAID-массивах серверов;
- жесткие диски, находящиеся в системных блоках АРМ ИС;
- кассеты со стримерными лентами, находящиеся в стримерных устройствах;
- USB-носители, находящиеся у пользователей ИС и содержащие резервные копии;
- CD-R, CD-RW, DVD-R и/или DVD-RW-носители,

подлежат регистрации и учету.

Учетный номер носителя, содержащего защищаемую информацию, должен наноситься непосредственно на корпус носителя и быть нестираемым.

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

Запрещено использование в ИС неучтенных машинных носителей информации для обработки защищаемой информации.

Регистрация действий по подключению к ИС машинных носителей информации осуществляется в электронных журналах СЗИ от НСД.

Запрещается копирование защищаемой информации пользователями ИС с целью их передачи другим сотрудникам или посторонним лицам.

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

Полученные извне машинные носители информации, содержащие необходимую для деятельности защищаемую информацию, должны:

- проверяться на наличие вредоносных программных продуктов;
- учитываться в соответствии с настоящей политикой;
- передаваться сотрудникам, являющимся пользователями ИС, только с

разрешения руководителя структурного подразделения с записью в соответствующих формах учета.

Регистрацию и учет машинных носителей защищаемой информации для каждой ИС осуществляет администратор информационной безопасности в соответствующем журнале учета машинных носителей информации, форма которого приведена в Приложении № 7 к настоящему Положению.

17.2. Порядок хранения машинных носителей защищаемой информации

Хранение машинных носителей защищаемой информации осуществляется в условиях, исключающих утрату их функциональности и хранимой информации из-за

влияния внешних полей, излучений и иных неблагоприятных факторов, а также НСД к защищаемой информации.

Машинные носители защищаемой информации должны храниться в недоступном для посторонних лиц месте: в шкафах, оборудованных замками.

17.3. Порядок эксплуатации машинных носителей защищаемой информации

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

Передача машинных носителей защищаемой информации для ремонта или утилизации запрещена.

Все машинные носители защищаемой информации, потерявшие актуальность, передаются администратору информационной безопасности. По результатам уничтожения защищаемой информации с машинного носителя или форматирования машинного носителя, или уничтожения машинного носителя составляется акт об уничтожении защищаемой информации и/или акт об уничтожении машинного носителя защищаемой информации. По факту уничтожения машинного носителя защищаемой информации в журнале учета машинных носителей информации производится отметка об уничтожении.

18. Организация резервирования и восстановления информации в ИС

18.1. Общие положения

С целью обеспечения возможности незамедлительного восстановления защищаемой информации в ИС, модифицированной или уничтоженной вследствие НСД к ней или возникновении нештатных ситуаций, повлекших за собой потерю данных, организуется резервирование и восстановление информации в ИС, а также работоспособности ИС.

18.2. Информация, подлежащая резервному копированию

Резервному копированию подлежат следующие информационные ресурсы:

- файлы, каталоги, БД ИС, содержащие защищаемую информацию;
- системные и конфигурационные файлы ОС и специального ПО серверов;
- конфигурационные файлы сетевого оборудования;
- системные и конфигурационные файлы СЗИ.

18.3. Порядок резервирования и хранения резервных копий

Резервное копирование защищаемой информации должно осуществляться ЕЖЕМЕСЯЧНО на машинные носители информации, создавая тем самым резервный электронный архив. Факт резервного копирования подлежит обязательной регистрации в соответствующем журнале резервного копирования информационных массивов информационных систем, форма которого приведена в Приложении № 8 к настоящему Положению.

Машинные носители информации, на которые осуществляется резервное копирование защищаемой информации, должны быть поставлены на соответствующий учет и зарегистрированы в журнале учета машинных носителей информации.

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.

Машинные носители информации с обновлениями ПО маркируют датой их получения (датой выхода обновления).

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.

18.4. Порядок восстановления работоспособности информационной системы

В случае возникновения нештатной ситуации, вызвавшей полную или частичную потерю работоспособности ИС, должно быть обеспечено ее восстановление из резервной копии. Факт возникновения нештатной ситуации в ИС подлежит обязательной регистрации в журнале учета нештатных ситуаций в информационных системах, форма которого приведена в Приложении № 9 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, в результате сбоев в сети электропитания.

Восстановление СЗИ производится с использованием дистрибутива. Дистрибутив может быть получен как на машинном носителе информации, так и с официального сайта производителя (разработчика). Порядок получения дистрибутива СЗИ устанавливается производителем (разработчиком).

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 учетный машинный носитель информации.

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

19. Порядок работы с электронными журналами протоколирования и анализа (аудита) значимых событий (регистрация событий безопасности)

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

Источники событий безопасности, подлежащих регистрации в соответствующих электронных журналах:

- СЗИ;
- программное обеспечение ИС и СУБД;
- общесистемное и прикладное ПО.

Перечень событий безопасности, подлежащих фиксации СЗИ:

1) Регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

2) Регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ.

3) Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный).

4) Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла.

5) Регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)].

Проверка электронного журнала событий СЗИ от НСД производится в соответствии с прилагаемой к ним технической и эксплуатационной документацией.

Срок хранения электронного журнала событий СЗИ от НСД должен быть не менее 1 (Одного) года.

СЗИ от НСД должно сигнализировать администратору информационной безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности. В этом случае администратор информационной безопасности должен предпринять меры для устранения возникшего сбоя с учетом требований настоящего Положения и технической и эксплуатационной документации на СЗИ от НСД.

Для всех АРМ в составе ИС должна быть обеспечена синхронизация системного времени.

Администратор информационной безопасности должен еженедельно осуществлять анализ электронных журналов:

- СЗИ;
- программное обеспечение ИС и СУБД;
- общесистемное и прикладное ПО

с обязательной регистрацией в журнале проверки электронных журналов информационных систем, форма которого приведена в Приложении № 10 к настоящему Положению.

20. Порядок обращения со средствами защиты информации

20.1. Учет средств защиты информации

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

Процедура установки СЗИ сопровождается оформлением акта установки СЗИ, форма которого приведена в Приложении № 14 к настоящему Положению. В случае необходимости деинсталляции СЗИ оформляется соответствующая заявка, форма которой приведена в Приложении № 15 к настоящему Положению. Процедура деинсталляции СЗИ сопровождается оформлением акта деинсталляции СЗИ, форма которого приведена в Приложении № 16 к настоящему Положению.

Инсталлирующие СЗИ носители, установленные СЗИ, эксплуатационная и техническая документация к СЗИ подлежат поэкземплярому учету в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним, форма которого приведена в Приложении № 11 к настоящему Положению.

Администратор информационной безопасности должен осуществлять один раз в месяц тестирование СЗИ с отметкой в журнале учета периодического тестирования средств защиты информации информационных систем, форма которого приведена в Приложении № 12.

20.2. Распространение средств защиты информации

СЗИ доставляются фельдъегерской (в том числе ведомственной) связью или со специально выделенными сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к СЗИ во время доставки.

При пересылке СЗИ помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. Эксплуатационная и техническая документация к СЗИ пересылается заказными, ценными почтовыми отправлениями или доставляется специально выделенными сотрудниками.

При пересылке СЗИ, эксплуатационной и технической документации к ним подготавливается сопроводительное письмо, в котором указывается: что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывается в одну из упаковок.

Отправитель контролирует доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель направляет ему запрос и принимает меры к уточнению местонахождения отправлений.

20.3. Получение средств защиты информации

Полученные упаковки вскрываются только лицом, для которого они предназначены.

Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать – их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получателем составляется акт, который высылается отправителю. Полученные с такими отправлениями СЗИ до получения указаний от отправителя применять не разрешается.

При обнаружении бракованных СЗИ один экземпляр бракованного изделия возвращается отправителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранятся до поступления дополнительных указаний от отправителя.

Получение СЗИ, эксплуатационной и технической документации к ним подтверждается отправителю в соответствии с порядком, указанным в сопроводительном письме.

20.4. Уничтожение средств защиты информации

СЗИ уничтожаются (утилизируются) по решению директора.

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.

Уничтожение большого объема инсталлирующих СЗИ носителей оформляется актом. Уничтожение по акту производится комиссией в составе не менее трех человек из числа лиц, допущенных к работе с СЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых инсталлирующих СЗИ носителей. Исправления в тексте акта оговариваются и заверяются подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним.

Эксплуатационная и техническая документация к СЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин. Факт уничтожения эксплуатационной и технической документации к СЗИ оформляется в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним.

Уничтожение большого объема эксплуатационной и технической документации к СЗИ оформляется актом. Уничтожение по акту производится

комиссией в составе не менее трех человек из числа лиц, допущенных к работе с СЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемой эксплуатационной и технической документации к СЗИ. Исправления в тексте акта оговариваются и заверяются подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в журнале поэкземплярного учета средств защиты информации информационных систем, эксплуатационной и технической документации к ним.

20.5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства защиты информации

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СЗИ, должны обеспечивать сохранность ПДн, СЗИ, исключать возможность неконтролируемого проникновения или пребывания в помещениях, где установлены СЗИ, посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

При оборудовании помещений, где установлены СЗИ, должны выполняться требования к размещению и монтажу СЗИ, а также другого оборудования, функционирующего с СЗИ.

Инсталлирующие СЗИ носители, эксплуатационная и техническая документация к СЗИ должна храниться в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Помещения, где установлены СЗИ, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Для предотвращения просмотра извне помещений, где установлены СЗИ, их окна должны быть оборудованы шторами или жалюзи.

20.6. Ответственность за нарушение требований эксплуатации средств защиты

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

Пользователи ИС несут персональную ответственность за сохранность полученных СЗИ, эксплуатационной и технической документации к СЗИ, за соблюдение положений настоящего Положения.

Администратор информационной безопасности несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки ПДн с использованием СЗИ лицензионным требованиям и условиям, эксплуатационной и технической документации к СЗИ.

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

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

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

Ответственность за невыполнение требований настоящей главы, проведение в плановом порядке работ по обновлению оборудования, операционной системы, 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 ИС при внесении изменений и дополнений в ПО и оборудование на отсутствие негативных воздействий на функционирование ИС, ответственность за мониторинг событий, фиксируемых системами безопасности, несет администратор информационной безопасности.

Установке нового оборудования предшествует тестирование инфраструктуры ИС и критических приложений на отсутствие негативных воздействий вновь устанавливаемого оборудования.

Установке обновлений предшествует тестирование информационной инфраструктуры ИС на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

При обнаружении негативного воздействия устанавливаемого оборудования на инфраструктуру ИС, 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 информационной инфраструктуры ИС 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.

22. Управление конфигурацией информационной системы и ее системы защиты

Администратор информационной безопасности организует управление конфигурацией ИС и ее системы защиты информации в соответствии с требованиями настоящего раздела.

Под конфигурацией ИС и ее системы защиты информации понимается совокупность следующих характеристик:

- состав программного и аппаратного обеспечения ИС;
- места размещения технических средств ИС;
- параметры настройки программного обеспечения и технических средств информационной системы;
- структура системы защиты информации;
- состав, места установки и параметры настройки средств защиты информации.

Администратор информационной безопасности организует проверку текущей конфигурации ИС и ее системы защиты на соответствие базовой конфигурации. Результат проверки оформляется Актом контроля текущей конфигурации (Приложение № 17).

Внесение изменений в конфигурацию ИС и ее системы защиты осуществляется по согласованию с администратором информационной безопасности с обязательной отметкой в журнале регистрации действий по сопровождению информационных систем и изменению их конфигураций, форма которого приведена в Приложении № 18.

В случае внесения изменений в конфигурацию аттестованной по требованиям защиты информации ИС и ее системы защиты может возникнуть необходимость согласования изменений с соответствующей организацией-лицензиатом ФСТЭК России.

Требования настоящего раздела направлены на предотвращение:

- нарушения штатной работы информационных ресурсов и сервисов ИС;
- нарушения штатного функционирования оборудования;
- несанкционированного уничтожения защищаемой информации;
- несанкционированной модификации защищаемой информации;
- несанкционированного копирования защищаемой информации.

Установка нового оборудования в составе ИС.

Установке нового оборудования предшествует тестирование инфраструктуры ИС и критических приложений на отсутствие негативных воздействий вновь устанавливаемого оборудования.

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

Установка (обновление) программного обеспечения.

Установке обновлений ПО, новых версий ПО и дополнений в действующее ПО предшествует тестирование информационной инфраструктуры ИС на отсутствие негативных воздействий от вновь устанавливаемого ПО (обновлений ПО).

При обнаружении негативного воздействия устанавливаемого ПО (обновлений ПО) на инфраструктуру ИС, функционирующую в штатном режиме, такое ПО (обновление ПО) не устанавливается. В этом случае разрабатывается план дополнительных мероприятий, направленных на устранение негативного воздействия устанавливаемого ПО (обновления ПО).

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

Конфигурация ИС и ее системы защиты фиксируется в эксплуатационной документации ИС. Актуализация эксплуатационной документации осуществляется администратором информационной безопасности по факту принятия решения о внесении соответствующих изменений.

23. Анализ защищенности информации при ее обработке в ИС

Администратор информационной безопасности должен ежемесячно осуществлять тестирование работоспособности СЗИ штатными средствами с отметкой в журнале учета периодического тестирования средств защиты информации информационных систем, форма которого приведена в Приложении № 12.

Администратор информационной безопасности несет ответственность за анализ защищенности информации при ее обработке в ИС, в том числе:

- отслеживание появления новых уязвимостей программного обеспечения и оборудования, используемых в составе ИС;
- проведение в плановом порядке работ по обновлению оборудования, общесистемного и прикладного программного обеспечения, программного обеспечения средств защиты информации в целях своевременной ликвидации выявленных уязвимостей;
- предварительное тестирование ИС при внесении изменений и дополнений в ПО и оборудование на отсутствие негативных воздействий на функционирование ИС (в соответствии с требованиями главы «Управление конфигурацией информационной системы и ее системы защиты» настоящего Положения);
- мониторинг событий, фиксируемых средствами защиты информации.

24. Выявление инцидентов безопасности и реагирование на них

24.1. Общие сведения

Инциденты безопасности – непредвиденные или нежелательные события, которые могут нарушить работоспособность ИС или безопасность защищаемой информации:

- отказ в обслуживании;
- длительные нарушения в работе технических средств, программного обеспечения и (или) средств защиты информации;
- нарушение правил разграничения доступа;
- неправомерные действия по сбору информации;
- внедрение вредоносных компьютерных программ (вирусов);
- выявление признаков инцидентов безопасности при анализе журналов событий;
- иные события, приводящих к реализации угроз информационной безопасности.

Источниками информации об инцидентах безопасности для ИС являются:

- факты, выявленные сотрудниками МАОУ СОШ № 50;
- результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов/АРМ/ ОС/гостевых ОС, антивирусной системы, системы резервного копирования и других подсистем безопасности;
- обращения субъектов персональных данных с указанием инцидента безопасности;
- сообщения Федеральной службы технического и экспортного контроля Российской Федерации;
- сообщения Федеральной службы безопасности Российской Федерации;
- сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;
- иные источники информации.

Основные виды инцидентов безопасности:

- несанкционированный доступ к информационным ресурсам ИС;
- разглашение защищаемой информации либо угроза такого разглашения;
- превышение полномочий – несанкционированный доступ к каким-либо ресурсам и помещениям;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- сетевые атаки (отказ в обслуживании), атаки типа Man-in-the-Middle, sniffing пакетов, переадресация портов, IP-спуфинг, атаки на уровне приложений и другое.

24.2. Обнаружение, идентификация и регистрация инцидентов безопасности

Выявление инцидентов безопасности и реагирование на них включает в себя следующие мероприятия:

- регламентация правил и процедур реагирования на инциденты безопасности, в том числе определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение, идентификация и регистрация инцидентов безопасности;
- своевременное информирование лиц, ответственных за выявление инцидентов безопасности и реагирование на них, о возникновении инцидентов безопасности;
- анализ инцидентов безопасности, в том числе определение источников и причин возникновения инцидентов безопасности, а также оценка их последствий;
- принятие мер по устранению последствий инцидентов безопасности;
- планирование и принятие мер по предотвращению повторного возникновения инцидента безопасности;
- хранение и защита информации об инцидентах безопасности.

Обнаружение инцидентов безопасности включает в себя мероприятия, направленные на:

- 1) выявление инцидентов безопасности с помощью технических средств;
- 2) выявление инцидентов безопасности в ходе контрольных мероприятий.

При получении информации о несанкционированном воздействии на инфраструктуру ИС администратор информационной безопасности обязан убедиться, что инцидент безопасности не является результатом собственной ошибки или санкционированных действий.

Лицо, обнаружившее инцидент, должно незамедлительно, любым доступным способом, сообщить об инциденте администратору информационной безопасности, который принимает решение о необходимости информирования пользователей ИС о возникновении инцидента безопасности и дает указания по дальнейшим действиям.

Администратор информационной безопасности учитывает инциденты безопасности в журнале учета нештатных ситуаций в информационных системах, форма которого приведена в Приложении № 9 к настоящему Положению, информирует об инциденте другие структурные подразделения.

Перечень действий при реагировании на инциденты безопасности, реализуемые администратором информационной безопасности:

- принятие мер по устранению инцидентов безопасности;
- анализ инцидентов безопасности, в том числе определение источников и причин возникновения инцидентов безопасности, а также оценка их последствий;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов безопасности.

24.3. Планирование и принятие мер по предотвращению инцидентов безопасности

Планирование и принятие мер по предотвращению возникновения инцидентов безопасности осуществляется администратором информационной безопасности и основывается на:

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками МАОУ СОШ № 50;
- проведении мероприятий по обучению сотрудников МАОУ СОШ № 50 правилам и способам работы со средствами защиты;
- доведении до сотрудников МАОУ СОШ № 50 норм законодательства, локальных актов по вопросам информационной безопасности и устанавливающих ответственность за нарушение требований информационной безопасности;
- разъяснительной работе с лицами, принимаемыми на работу, и увольняющимися сотрудниками;
- своевременной модернизации системы обеспечения информационной безопасности с учетом возникновения новых угроз информационной безопасности и при изменении требований законодательных актов и нормативных документов по защите информации;
- своевременном обновлении ПО, в том числе ПО СЗИ и средств криптографической защиты информации.

24.4. Реагирование на инциденты, повлекшие неправомерную передачу (предоставление, распространение, доступ) персональных данных

МАОУ СОШ № 50 обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – ГосСОПКА), включая его информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн.

В случае установления МАОУ СОШ № 50 факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, обрабатываемых в МАОУ СОШ № 50, повлекшей нарушение прав субъектов ПДн:

- директор МАОУ СОШ № 50 _инициирует проведение внутреннего расследования выявленного инцидента;
- директор МАОУ СОШ № 50 __утверждает состав комиссии, участвующей в внутреннем расследовании выявленного инцидента;
- комиссия проводит внутреннее расследование выявленного инцидента;
- результатом работы комиссии является акт внутреннего расследования выявленного инцидента, содержащий:
 - состав комиссии;
 - период времени, в течение которого проводилась служебная проверка;
 - основание проведения служебной проверки;

- документальное подтверждение фактов нарушений, выявленных в ходе расследования и имеющих значение в определении наличия нарушений, а также иных фактов, которые могут привести к нарушению конфиденциальности защищаемой информации или к снижению уровня защищенности ПДн;

- установленные причины выявленного инцидента;
- сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии);
- сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии), и причинах, допустивших наступление инцидента;
- сведения о предполагаемом вреде, нанесенном правам субъектов ПДн;
- сведения о принятых мерах по устранению последствий соответствующего инцидента;
- рекомендации по совершенствованию системы обеспечения безопасности ПДн, исключая в дальнейшем подобный инцидент.

Администратор информационной безопасности обязан с момента выявления такого инцидента МАОУ СОШ № 50, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов ПДн в соответствии с Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 г. № 187:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, сведения о лице, уполномоченном МАОУ СОШ № 50 на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом, сведения об Операторе;
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Передача указанной информации Роскомнадзором в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) регламентируется порядком, устанавливаемым ФСБ России и Роскомнадзором в соответствии с частью 11 статьи 23 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Оператор вправе обратиться в НКЦКИ для оказания содействия в реагировании на выявленный компьютерный инцидент, повлекший неправомерную передачу (предоставление, распространение, доступ) персональных данных и привлечения сил ГосСОПКА.

25. Правила и процедуры информирования и обучения персонала

25.1. Цели и задачи обучения вопросам информационной безопасности

Цель обучения персонала – формирование и поддержание необходимого уровня квалификации сотрудников МАОУ СОШ № 50 с учетом требований в сфере информационной безопасности и обеспечения требуемого уровня защищенности информации в ИС.

Задачи в области обучения вопросам информационной безопасности:

- выработка и соблюдение правил по защите информации в ИС;
- разработка и внедрение системы обучения, включающей выявление потребности в обучении, планирование и бюджетирование, организацию обучения и контроль его результативности;
- включение передового опыта, знаний, эффективных методов организации труда в процессе обучения сотрудников вопросам информационной безопасности;
- мотивация сотрудников к повышению безопасности и обеспечению надежности работы;
- регулярная проверка знаний в сфере информационной безопасности и их применение на практике.

25.2. Виды обучения и проверки знаний

По формам планирования, организации обучения и проверки знаний подразделяются на плановые и внеплановые:

- а) Плановые – проводятся по программам обучения:
 - Вводный инструктаж: проводится при поступлении лица на работу в МАОУ СОШ № 50;
 - Первичный инструктаж на рабочем месте: проводится при выполнении работ, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности;
 - Первичная проверка знаний: проводится не позднее трех месяцев после назначения на должность;
 - Повторное обучение: проводится для сотрудников МАОУ СОШ № 50, выполняющих работы, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности, проводится один раз в три года.
- б) Внеплановые – проводятся по производственной необходимости, а также по заявкам руководителей структурных подразделений. Форма заявки приведена в Приложении № 19 к настоящему Положению:
 - Внеочередное обучение: проводится при изменении требований по информационной безопасности, изменениях в бизнес-процессах или при нарушениях информационной безопасности;
 - Внеплановая проверка знаний: проводится при изменении требований к информационной безопасности, изменениях в бизнес-процессах или при нарушениях информационной безопасности, проводится не реже одного раза в три года;

– Целевое обучение: проводится при выполнении разовых работ, не связанных с прямыми обязанностями сотрудников;

– Специальное обучение: проводится при выполнении работ, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности.

По формам проведения обучение и проверки знаний подразделяются на индивидуальные и корпоративные (групповые), внутренние и внешние:

– Индивидуальное обучение: проводится с сотрудником МАОУ СОШ № 50 персонально;

– Корпоративное (групповое): организация групп или обучение одновременно нескольких сотрудников одного подразделения;

– Внешнее: проводится с привлечением внешних образовательных организаций.

25.3. Организация обучения и проверки знаний

В ходе информирования и обучения персонала осуществляется:

– информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации ИС;

– доведение до персонала требований по обеспечению безопасности ИС, а также положений организационно-распорядительных документов по информационной безопасности в части, их касающейся;

– обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;

– контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности.

Обучение и проверка знаний в порядке, установленном настоящим документом, распространяется на:

– руководителей и сотрудников структурных подразделений, которые:

- осуществляют эксплуатацию ИС;
- обеспечивающие функционирование (сопровождение, обслуживание, ремонт) технических и программных компонентов ИС;

– временных сотрудников;

– работников, выполняющих работы, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности.

Ответственность за организацию своевременного и качественного обучения и проверки знаний по информационной безопасности возлагается на администратора информационной безопасности.

Обучение и инструктаж по информационной безопасности должен проводиться в рабочее время.

Внеочередное обучение и проверка знаний по информационной безопасности руководителей и сотрудников проводится независимо от срока проведения предыдущего обучения и проверки в следующих случаях:

- при введении в действие новых нормативных документов по информационной безопасности или вступления в законную силу изменений в нормативные документы по информационной безопасности;

- при изменениях технологических процессов и замене оборудования, требующих дополнительных знаний по информационной безопасности обслуживающего персонала;

- при назначении или переводе на другую работу, если новые обязанности требуют от руководителей и сотрудников дополнительных знаний по информационной безопасности (до начала исполнения своих обязанностей);

- по требованию руководителей подразделений при установлении недостаточных знаний;

- после наступления инцидентов безопасности, нештатных ситуаций, при повышении вероятности осуществления потенциальными нарушителями угроз информационной безопасности;

- при совершенных нарушениях требований нормативных документов по информационной безопасности руководителями и сотрудниками МАОУ СОШ № 50;

- при возникновении перерыва в работе в данной должности более одного года.

Непосредственно перед очередной (внеочередной) проверкой знаний по информационной безопасности руководителей и сотрудников МАОУ СОШ № 50 могут проводиться:

- специальная подготовка с целью углубления знаний по наиболее важным вопросам информационной безопасности;

- семинары;

- консультации.

О дате и месте проведения проверки знаний сотрудник должен быть предупрежден не позднее чем за 15 рабочих дней.

Для проведения проверки знаний по информационной безопасности приказом создаются комиссии по проверке знаний. Состав, порядок и форма работы комиссий по проверке знаний определяется МАОУ СОШ № 50.

Факт проведения обучения, проверки знаний фиксируются в журнале проведения обучения и проверки знаний по вопросам информационной безопасности, форма которого приведена в Приложении № 20 к настоящему Положению.

Внешнее обучение по вопросам информационной безопасности руководителей и сотрудников проводится по программам, разработанным и утвержденным учебными центрами, организациями, институтами, имеющими лицензии на обучение в данной сфере знаний.

26. Правила и процедуры планирования мероприятий по обеспечению безопасности

26.1. Основные цели планирования

Основными целями планирования мероприятий по защите информации в ИС являются:

- организация проведения комплекса мероприятий по обеспечению безопасности защищаемой информации, направленных на исключение возможных каналов утечки информации;
- установление персональной ответственности должностных лиц за решение вопросов защиты информации в ходе эксплуатации ИС;
- определение сроков (времени, периода) проведения конкретных мероприятий по защите информации;
- систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты информации;
- установление системы контроля за обеспечением защиты информации в ИС, а также системы отчетности о выполнении конкретных мероприятий;
- уточнение, конкретизация функций и задач, решаемых отдельными должностными лицами и/или структурными подразделениями.

Подтверждением проведения контрольных мероприятий является:

- меры, средства и мероприятия, проводимые в целях защиты информации, обеспечивают поддержание уровня защищенности информации в ИС;
- система защиты информации обеспечивает защиту информации при эксплуатации ИС;
- средства защиты информации настроены и используются в соответствии с техническими условиями, правилами эксплуатации и требованиями формуляров;
- рекомендации предшествующих проверок реализованы в полной мере.

26.2. Планирование контрольных мероприятий

Контрольные мероприятия (проверки) проводятся МАОУ СОШ № 50 на плановой основе, а также внепланово. Внеплановые проверки проводятся по фактам выявления сотрудниками _ МАОУ СОШ № 50 нарушений функционирования элементов ИС и инцидентов информационной безопасности, при существенных изменениях в среде обработки защищаемой информации.

Плановые проверки проводятся на периодической основе и включают:

- проверку актуальности нормативно-организационных документов;
- проверку работоспособности и эффективности технических средств ИС;
- проверку соответствия предъявляемых мер защиты к предъявляемым характеристикам ИС по требованиям безопасности информации (уровню защищенности информации в ИС);
- проверку деятельности персонала МАОУ СОШ № 50, эксплуатирующего ИС, на соответствие требований к обеспечению безопасности ИС;

- проверку компетентности персонала, задействованного в обслуживании системы защиты ИС;
- проверку управления инцидентами в ИС;
- контроль модернизации системы безопасности ИС;
- контроль обеспечения бесперебойной эксплуатации ИС.

Для проведения контрольных мероприятий администратор информационной безопасности разрабатывает ежегодный план мероприятий по обеспечению безопасности ИС и представляет его на утверждение директору МАОУ СОШ № 50 (далее – план мероприятий). План мероприятий может быть включен в сводный план мероприятий по обеспечению безопасности, утверждаемый МАОУ СОШ № 50.

План мероприятий должен содержать:

- перечень мероприятий по обеспечению безопасности;
- сроки проведения мероприятий;
- состав подразделений (работников), ответственных за реализацию каждого мероприятия.

Контроль за выполнением плана мероприятий осуществляется специалистом, ответственным за защиту информации, который ежегодно готовит отчет о выполнении плана мероприятий, который представляется директору МАОУ СОШ № 50.

Контроль состояния безопасности проводится ежегодно. Различают внешний и внутренний контроль состояния безопасности. Внутренний контроль включает плановые и внеплановые проверки, указанные выше.

Внутренний контроль проводится комиссией, назначаемой директором МАОУ СОШ № 50. В состав комиссии входят: администратор информационной безопасности; сотрудники иных заинтересованных подразделений. Результат внутреннего контроля оформляется протоколом, который подписывается членами комиссии и утверждается директором МАОУ СОШ № 50 (Приложение № 21).

Внешний контроль (аудит) проводится внешней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

26.3. Оформление результатов контрольных мероприятий

Факты проведения плановых или внеплановых контрольных мероприятий МАОУ СОШ № 50 фиксируются в журнале учета проведения внутреннего контроля за обеспечением уровня защищенности информации (Приложение № 13).

По итогам проведения контрольных мероприятий администратор информационной безопасности разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения контрольного мероприятия.

27. Ответственность за нарушение требований законодательства

Должностные лица, ответственные за организацию работ по защите информации и непосредственное выполнение указанных работ назначаются локальными актами Оператора.

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

УТВЕРЖДАЮ_____
(должность)_____
(фамилия, имя, отчество)

«__» _____ 20__ г.

М.П.

Акт № _____
об уничтожении защищаемой информации

Комиссия в составе:

председатель комиссии

(должность, Фамилия Имя Отчество)

члены комиссии

(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 персональных данных.

№ 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 ПДн)

Председатель комиссии

(Фамилия Имя Отчество)_____
(подпись)

Члены комиссии

(Фамилия Имя Отчество)_____
(подпись)_____
(Фамилия Имя Отчество)_____
(подпись)

Муниципальное автономное
 общеобразовательное учреждение
 средняя общеобразовательная школа
 с углубленным изучением отдельных
 предметов № 50.

Приложение № 2 –Б

УТВЕРЖДАЮ

_____ (должность)

_____ (фамилия, имя, отчество)

«__» _____ 20__ г.

М.П.

Акт № _____
 об уничтожении персональных данных

Комиссия в составе:

председатель комиссии

_____ (должность, Фамилия Имя Отчество)

члены комиссии

_____ (должность, Фамилия Имя Отчество)

_____ (должность, Фамилия Имя Отчество)

подтверждает уничтожение персональных данных в соответствии с таблицей:

№ п/п	ФИО субъекта	Категория ПДн	Наименование ИСПДн ¹	Материальный носитель, кол-во страниц ²	Способ	Причина

Уничтожение произведено «__» _____ 20__ г.

Приложение¹: Выгрузка из журнала регистрации событий в информационной системе персональных данных **%Наименование ИСПДн%**.

Председатель комиссии

_____ (Фамилия Имя Отчество)

/ _____ / (подпись)

Члены комиссии

1 – при автоматизированной обработке персональных данных.

2 – при обработке персональных данных без использования средств автоматизации.

1

(Фамилия Имя Отчество)

(Фамилия Имя Отчество)

(подпись)

/ _____ /

(подпись)

УТВЕРЖДАЮ_____
(должность)_____
(фамилия, имя, отчество)

«__» _____ 20__ г.

М.П.

**Акт № _____
об уничтожении машинных носителей информации**

Комиссия в составе:

– председатель комиссии _____

(должность, Фамилия Имя Отчество)

– члены комиссии _____

(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 машинных носителей информации)

Председатель
комиссии _____

(Фамилия Имя Отчество)

/ _____ /
(подпись)

Члены комиссии _____

(Фамилия Имя Отчество)

/ _____ /
(подпись)

(Фамилия Имя Отчество)

/ _____ /
(подпись)

1 – при автоматизированной обработке персональных данных.

2 – при обработке персональных данных без использования средств автоматизации.

**Форма заявки
на предоставление пользователю прав доступа**

к ИС/ИСПДн (ресурсу ИС/ИСПДн) _____

(наименование ИС/ ИСПДн или ресурса ИС/ ИСПДн)

№ п/п	Ф.И.О., № кабинета	Должность	Имя АРМ в домене	Права доступа к ИС/ИСПДн (ресурсу ИС/ИСПДн)			Время доступа к ИС/ИСПДн (ресурсу ИС/ИСПДн)	
				чтение	редактирование	удаление	дни недели	рабочие часы
1	2	3	4	5	6	7	8	9

Руководитель структурного подразделения _____

(подпись, расшифровка подписи)

« __ » _____ 20__ г.

Форма акта
установки средства защиты информации

АКТ
установки средства защиты информации

№ _____

« ____ » _____ 20__ г.

Рабочая группа в составе:

_____	_____
<i>(должность)</i>	<i>(Фамилия, Имя, Отчество)</i>
_____	_____
<i>(должность)</i>	<i>(Фамилия, Имя, Отчество)</i>
_____	_____
<i>(должность)</i>	<i>(Фамилия, Имя, Отчество)</i>

составила настоящий акт о том, что на основании заявки/служебной записки _____

(№, дата документа)

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	<i>Приводятся сведения о техническом средстве (например, системный блок, моноблок), на жесткий диск которого установлено СЗИ</i>		
2	<i>Приводятся сведения о жестком диске, на который установлено СЗИ</i>		

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

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)

Форма заявки
на деинсталляцию средства защиты информации

ЗАЯВКА
на деинсталляцию средства защиты информации

Прошу деинсталлировать средство защиты информации _____

(наименование средства защиты информации)

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

(должность, фамилия, имя, отчество пользователя СЗИ)

в связи с _____

(причина деинсталляции средства защиты информации)

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		

(должность)

(подпись)

(расшифровка подписи)

Форма акта
деинсталляции средства защиты информации
АКТ
деинсталляции средства защиты информации

№ _____

« ____ » _____ 20__ г.

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	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)

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

Пользователь СЗИ:

(должность, подпись, расшифровка подписи)

АКТ № _____
контроля текущей конфигурации ИС _____ и ее средств защиты
информации

« ____ » _____ 20__ г.

1. Отклонения в составе ИС:

2. Отклонения в составе системы защиты информации:

3. Отклонения в подключениях технических средств ИС и системы защиты информации:

4. Отклонения в составе программного обеспечения:

5. Отклонения в технологии обработки информации:

6. Выводы:

(должность, Ф.И.О.)

(подпись)

Форма журнала
учета регистрации действий по сопровождению информационных систем и
изменению их конфигураций

№ п/п	Дата и номер заявки на внесение изменений	Дата сопровождения/внесения изменений	Описание выполненных действий	Ф.И.О. и подпись ответственного лица,	Дата и номер акта контроля текущей конфигурации и ее средств защиты информации	Примечание
1	2	3	4	5		6

Форма заявки
на проведение обучения вопросам информационной безопасности

Подразделение	
Должность	
Фамилия И.О.	
Внутренний телефон	
Номер комнаты	

Провести обучение по следующим темам:

Тема	Дата

Привлечь специалистов для обучения по следующим темам:

Тема	Дата

Провести обучение во внешних организациях по следующим темам:

Тема	Дата

Должность: _____

(подпись)

(Ф.И.О.)

Форма журнала
проведения обучения и проверки знаний по
вопросам информационной безопасности

№ п/п	Дата	Вид обучение/ проверка знаний	Причина проведения обучения/проверки знаний	Ф.И.О., подпись обученного/проверенного	Ф.И.О., подпись обучающего/проверяю щего/название образовательной организации
1	2	3	4	5	6

Протокол
проведения внутреннего контроля
за обеспечением уровня защищенности информации

Настоящий Протокол составлен о том, что « ____ » _____ 20 ____ г.
_____ (комиссией)

(должность, Ф.И.О. должностного лица)

проведена проверка _____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями _____
(название документа)

В ходе проверки установлено: _____

Выявленные нарушения: _____

Меры по устранению нарушений: _____

Срок устранения нарушений: _____

Председатель комиссии:

(Ф.И.О.)

(подпись)

Члены комиссии:

(Ф.И.О.)

(подпись)

(Ф.И.О.)

(подпись)