

УТВЕРЖДЕЮ

Директор МАОУ СОШ № 132

Л.Г. Шевелева

Приказ № 417 от 28.08.2020



Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных МАОУ СОШ № 132

СОДЕРЖАНИЕ

1 Общие положения	3
2 Порядок подготовки к проведению контрольных мероприятий	4
Виды контрольных мероприятий.....	4
План проведения контрольных мероприятий.....	5
Оформление результатов проведенных контрольных мероприятий	5
3 Общий порядок проведения контрольных мероприятий	6
Контрольные мероприятия в подсистеме управления доступом.....	6
Контрольные мероприятия в подсистеме регистрации и учета.....	6
Контрольные мероприятия в подсистеме обеспечения целостности.....	8
Контрольные мероприятия в подсистеме антивирусной защиты.....	8
Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия.....	9
Контрольные мероприятия в подсистеме анализа защищенности.....	9
Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений	9
Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам.....	10
Контрольные мероприятия в подсистеме физической защиты	10
Контрольные мероприятия в подсистеме криптографической защиты.....	11
Приложение 1. Журнал учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн	

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных МАОУ СОШ №132 (далее—Регламент) устанавливает и определяет единый и обязательный порядок проведения контрольных мероприятий для каждой из подсистем, входящих в систему защиты персональных данных информационных систем персональных данных (далее -ИСПД МАОУ СОШ №132)

Настоящий Регламент утверждается и вводится руководителем МАОУ СОШ №132 и является обязательным для исполнения.

2 ПОРЯДОК ПОДГОТОВКИ К ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДМАОУ СОШ №132.

проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации МАОУ СОШ №132.

- и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

оценка уровня осведомленности и знаний работников МАОУ СОШ №132.

- в области обработки и защиты персональных данных (далее - ПД);

- оценка обоснованности и эффективности применяемых мер и средств защиты.

Виды контрольных мероприятий

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются силами работников МАОУ СОШ №132.

- ответственных за обеспечение безопасности ПД. При проведении внешних контрольных мероприятий привлекаются сторонние организации.

Кроме того, контрольные мероприятия подразделяются на плановые и внеплановые.

Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и направлены на постоянное совершенствование системы защиты персональных данных МАОУ СОШ №132.

Внеплановые контрольные мероприятия проводятся на основании решения инженера по безопасности группы информационных технологий. Решение о проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;

- по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

Кроме того любой работник МАОУ СОШ №132 вправе подготавливать обоснованные предложения о необходимости проведения внеплановых контрольных мероприятий и предоставить их лицу, ответственному за обеспечение безопасности ПД.

План проведения контрольных мероприятий

Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий,
- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий (см. раздел 2.3).

Оформление результатов проведенных контрольных мероприятий

По итогам проведения внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов в соответствии с планом;
- отклонения от плана, в случае их наличия;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений.
- заключение по итогам проведения внутреннего контрольного мероприятия.

Отчет передается на рассмотрение руководству МАОУ СОШ №132.

Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета мероприятий по обеспечению и контролю безопасности ПД, обрабатываемых в ИСПДМАОУ СОШ №132.(см. Приложение 1 настоящего Регламента).

3. ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПД, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы информационных систем, администраторы информационной безопасности.

Лицо, ответственное за обеспечение безопасности ПД, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

Контрольные мероприятия в подсистеме управления доступом

При проведении контрольных мероприятий в подсистеме управления доступом, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей работника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационных систем);
- проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа¹ (далее - НСД) при выполнении устанавливаемого числа неудачных попыток ввода пароля;
- проверка системы смены пароля принудительным образом (по истечению срока действия пароля);
- проверка выполнения требований по стойкости пароля.

Контрольные мероприятия в подсистеме регистрации и учета

При проведении контрольных мероприятий в подсистеме регистрации и учета, в зависимости от целей мероприятий, могут выполняться следующие проверки:

¹ Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой

- проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации и внутренних документах компании;

- имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;

- проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителем²;

- проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляция объектов).

Кроме того, при проведении проверок в части учета и хранения носителей персональных данных могут выполняться следующие проверки:

- проверка мест хранения носителей ПД, сейфов и металлических шкафов, надежность их замков;

- проверка выполнения установленного порядка учета и хранения носителей ПД;

- проверка фактического наличия всех носителей ПД, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенное хранение);

- проверка фактического наличия всех носителей ПД, переданных на архивное хранение;

- проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПД, независимо от даты их регистрации;

- проверка номенклатуры дел с целью выделения документов, содержащих ПД, для передачи в архив или на уничтожение;

- проверка правильности проставления регистрационных данных носителей, документов и дел, и учетных журналов;

- проверка правильности проставления в журнале отметок о движении носителей.

² Нарушитель (субъект атаки) – лицо (или иницируемый им процесс), проводящее (проводящий) атаку.

Контрольные мероприятия в подсистеме обеспечения целостности

При проведении контрольных мероприятий в подсистеме обеспечения целостности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
- проверка фактического наличия экземпляров резервных копий;
- проверка целостности сделанных резервных копий путем восстановления данных;
- имитация выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы.

Контрольные мероприятия в подсистеме антивирусной защиты

При проведении контрольных мероприятий в подсистеме антивирусной защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка рабочих станций и серверов станций на наличие установленных программных средств антивирусной защиты;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях;
- запуск полного сканирования системы в режиме реального времени антивирусным средством;
- проверка антивирусным средством используемых отчуждаемых носителей;
- проверка функционирования механизмов принудительной проверки используемых съемных носителей;
- имитация попыток заражения вредоносным программным обеспечением³ серверных и рабочих станций;

³ Вредоносное программное обеспечение - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия

При проведении контрольных мероприятий в подсистеме обеспечения безопасного межсетевого взаимодействия, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных межсетевых экранов требуемому уровню защищенности;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специального ПО;
- проверка системных журналов на наличие зафиксированных попыток обращения к «закрытым» ресурсам.

Контрольные мероприятия в подсистеме анализа защищенности

При проведении контрольных мероприятий в подсистеме анализа защищенности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка выполнения своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попыток НСД.

Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений

При проведении контрольных мероприятий в подсистеме обнаружения и предотвращения вторжений, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам

При проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка в помещениях, где ведется обработка ПД, установленных на окна жалюзи, штор и т.п.;
- проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т.п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные.

Контрольные мероприятия в подсистеме физической защиты

При проведении контрольных мероприятий в подсистеме физической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка введения журналов учета посетителей, проходящих на территорию МАОУ СОШ №132.
- проверка введения журналов посетителей, проходящих в защищаемые помещения;
- проверка электронных журналов СКУД на предмет попыток НСД в защищаемые помещения сотрудников, не имеющих права доступа в данные помещения;
- проверка наличия ключей (в том числе и электронных пропусков) от защищаемых помещений, а так же проверка сохранности вторых экземпляров ключей от защищаемых помещений;
- просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) по которым можно получить доступ в защищаемые помещения, а так же проверка принятых мер (блокирование электронного пропуска, смена замка);
- проверка надежности замков, установленных в защищаемых помещениях;
- имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управления доступом.

Контрольные мероприятия в подсистеме криптографической защиты

При проведении контрольных мероприятий в подсистеме криптографической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.
- проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографической защиты;
- проверка журналов учета средств криптографической защиты и используемых

криптоключей на правильность их ведения и хранения;

- проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения с криптоключами;

- проверка функционирования средств криптографической защиты путем имитации процессов, шифрования и дешифрования информации.

