УТВЕРЖДАЮ
Директор МБОУ СОШ № 23
_____ Н.В. Мокина
«29» августа 2019г.

Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации МБОУ СОШ№ 23

1ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент осуществления внутреннего контроля 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 информационных системах персональных данных МБОУ

СОШ №23 (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 -ИСПДн)МБОУСОШ №23 (далее –МБОУСОШ №23).

Настоящий Регламент утверждается и вводится руководителем МБОУСОШ №23и является обязательным для исполнения.

2ПОРЯДОК ПОДГОТОВКИ К ПРОВЕДЕНИЮ КОНТРОЛЬНЫХМЕРОПРИЯТИЙ

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 ИСПДнМБОУ СОШ №23 проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации образовательного МБОУСОШ №23 и действующего законодательства Российской Федерации в области обработки и защиты персональныхданных;
- оценка уровня осведомленности и знаний работников МБОУ СОШ №23 в области обработки и защиты персональных данных (далее -ПДн);
- оценка обоснованности и эффективности применяемых мер и средствзащиты.

2.1 Видыконтрольныхмероприятий

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются силами работников МБОУ СОШ №23, ответственных за обеспечение безопасности ПДн. 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 МБОУ СОШ №23.

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

- по результатам расследования инцидента информационнойбезопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

Кроме того любой работник МБОУ СОШ №23 вправе подготавливать обоснованные предложения о необходимости проведения внеплановых контрольных мероприятий и предоставить их лицу, ответственному за обеспечение безопасности ПДн.

2.2 Планпроведенияконтрольныхмероприятий

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:

- целипроведенияконтрольныхмероприятий;
- задачипроведенияконтрольныхмероприятий,

- объекты контроля (процессы, подразделения, информационные системы ит.п.);
- состав участников, привлекаемых для проведения контрольныхмероприятий;
- сроки и этапы проведения контрольныхмероприятий.

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).

2.3 Оформлениерезультатовпроведенныхконтрольныхмероприятий

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 спланом;
- отклонения от плана, в случае ихналичия;
- перечень и описание выявленныхнарушений;
- рекомендации по устранению выявленных нарушений.

заключение по итогам проведения внутреннего контрольного мероприятия. Отчет передается на рассмотрение руководству МБОУСОШ №23

Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн МБОУ СОШ №23 (см. Приложение 1 настоящего Регламента).

3.ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

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

Лицо, ответственное за обеспечение безопасности ПДн, 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.

3.1.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 обязанностейработника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационнойдокументации;
- проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационныхсистем);
- проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа[1] (далее - НСД) при выполнении устанавливаемого числа неудачных попыток вводапароля;
- проверка системы смены пароля принудительным образом (по истечению срока действияпароля);
- проверка выполнения требований по стойкостипароля.

3.2. Контрольные мероприятия в подсистеме регистрации иучета

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

- проверка системных журналов на наличие зарегистрированных попыток несанкционированногодоступа;
- 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 системномжурнале;
- проверка способов защиты системного журнала регистрации от уничтожения или модификациинарушителем[2];
- проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляцияобъектов).

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

- проверка мест хранения носителей ПДн, сейфов и металлических шкафов, надежность ихзамков;
- проверка выполнения установленного порядка учета и хранения носителейПДн;
- проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенноехранение);
- проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;
- проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПДн, независимо от даты ихрегистрации;
- проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или науничтожение;
- проверка правильности проставления регистрационных данных носителей, документов и дел, и учетныхжурналов;
- проверка правильности проставления в журнале отметок о движенииносителей.

3.3. Контрольные мероприятия в подсистеме обеспеченияцелостности

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 контрольныхсумм;

проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационнойдокументации;

- проверка целостности используемого программного обеспечения, путем вычисления контрольныхсумм;
- проверка фактического наличия экземпляров резервныхкопий;
- проверка целостности сделанных резервных копий путем восстановленияданных;
- имитациявыполнения резервного копирования и восстановления данных при аварийном режиме функционированиясистемы.

3.4.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 эксплуатационнойдокументации;
- проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверныхстанциях;
- запуск полного сканирования системы в режиме реального времени антивирусным средством;
- проверка антивирусным средством используемых отчуждаемыхносителей;
- проверка функционирования механизмов принудительной проверки используемых съемныхносителей;

- имитация попыток заражения вредоносным программным обеспечением[3] серверных и рабочихстанций;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоноснымПО.

3.5. 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 эксплуатационнойдокументации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специальногоПО;
- проверка системных журналов на наличие зафиксированных попыток обращенияк «закрытым» ресурсам.

3.6. Контрольные мероприятия в подсистеме анализазащищенности

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 данныхуязвимостей;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационнойдокументации;
- имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попытокНСД.

3.7. 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 эксплуатационнойдокументации.

3.8. 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 ПДн, установленных на окна жалюзи, штор ит.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 персональныеданные.

3.9. Контрольные мероприятия в подсистеме физическойзащиты

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

- проверка введения журналов учета посетителей, проходящих на территориюМБОУ СОШ №23*;*
- проверка введения журналов посетителей, проходящих в защищаемыепомещения;
- проверка электронных журналов СКУД на предмет попыток НСД в защищаемые

помещения сотрудников, не имеющих права доступа в данныепомещения;

- 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, сменазамка);
- проверка надежности замков, установленных в защищаемыхпомещениях;
- имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управлениядоступом.

3.10. Контрольные мероприятия в подсистеме криптографическойзащиты

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

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационнойдокументации.
- проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографическойзащиты;
- проверка журналов учета средств криптографической защиты и используемых криптоключей на правильность их ведения ихранения;
- проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения скриптоключами;
- проверка функционирования средств криптографической защиты путем имитации процессов, шифровании и дешифрованияинформации.

ПРИЛОЖЕНИЕ 1. ЖУРНАЛ УЧЕТА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ И КОНТРОЛЮ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В ИСПДН МБОУСОШ №23

УТВЕРЖДАЮ

_____

_____

«_____»_____20г.

ЖУРНАЛ

УЧЕТА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ И КОНТРОЛЮ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В ИСПДН »НО»

Журналначат«_____»_____20___г.

Должность

_____/ ФИО должностноголица /

Журналзавершен«_____»_____20___г.

Должность

_____/ ФИО должностного лица /

№ п/п	Наименование мероприятия, основание для проведения	Описаниемероприятия	Срокипроведения контрольных мероприятий		Составучастников	Объекты контроля	Выявленныенарушения, выданныерекомендации		Отметка о контроле устранения выявленных нарушений
			Датаначала	Дата окончания					
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**