Приложение № 13
к Политике в отношении
обработки персональных данных в
АУ СОН ТО и ДПО «РСРЦН «Семья»

РЕГЛАМЕНТ ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, А ТАКЖЕ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

ПОРЯДОК ПОДГОТОВКИ К ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Контрольные мероприятия ПО обеспечению уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдения требований законодательства Российской Федерации по обработке персональных данных в ИСПДн АУ СОН ТО И ДПО «РСРЦН «Семья» проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации АУ СОН ТО И ДПО «РСРЦН «Семья» и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценки уровня осведомленности и знаний сотрудников АУ СОН ТО И ДПО «РСРЦН «Семья» в области обработки и защиты персональных данных (далее - ПДн);
- оценка обоснованности и эффективности применяемых мер и средств защиты.

1.1 Виды контрольных мероприятий

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются сотрудниками АУ СОН ТО И ДПО «РСРЦН «Семья», ответственными за обеспечение безопасности ПДн. При проведении внешних контрольных мероприятий привлекаются сторонние организации.

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 совершенствование системы защиты персональных данных АУ СОН ТО И ДПО «РСРЦН «Семья».

Внеплановые контрольные мероприятия проводятся на основании решения руководителя АУ СОН ТО И ДПО «РСРЦН «Семья», либо сотрудника, назначенного ответственным за организацию обработки персональных данных. 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.

Любой сотрудник АУ СОН ТО И ДПО «РСРЦН «Семья» вправе вносить предложения о необходимости проведения внеплановых контрольных мероприятий.

1.1 План проведения контрольных мероприятий

Для проведения плановых внутренних контрольных мероприятий разрабатывается План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий 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.

1.1 Оформление результатов проведенных контрольных мероприятий

По итогам проведения внутренних контрольных мероприятий разрабатывается 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 ответственному за организацию обработки ПДн в АУ СОН ТО И ДПО «РСРЦН «Семья».

Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн АУ СОН ТО И ДПО «РСРЦН «Семья».

1 ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Контрольные мероприятия проводятся при обязательном участии сотрудника , ответственного за эксплуатацию ИСПДн, также могут привлекаться иные сотрудника АУ СОН ТО И ДПО «РСРЦН «Семья».

Сотрудник, назначенный ответственным за организацию обработки персональных данных, не позднее, чем за три рабочих дня до начала проведения контрольных мероприятий, уведомляет об этом всех ответственных за эксплуатацию ИСПДн АУ СОН ТО И ДПО «РСРЦН «Семья», в отношении которых планируется проведение контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

1.1 Контрольные мероприятия в подсистеме управления доступом

При проведении контрольных мероприятий в подсистеме управления доступом могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей сотрудника;
- 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 системы смены пароля принудительным образом (по истечению срока действия пароля);
- проверка выполнения требований по стойкости пароля.

1.1 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:

- 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 АУ СОН ТО И ДПО «РСРЦН «Семья»;
- имитация попытки несанкционированного доступа в систему для проверки работы системы регистрации;

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

При проведении проверок в части учета и хранения носителей персональных данных (далее - ПДн) могут выполняться следующие проверки:

- проверка мест хранения носителей ПДн, сейфов и металлических шкафов;
- проверка выполнения установленного порядка учета и хранения носителей ПДн;
- проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы;
- проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;
- проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение;

1.1 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 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.

1.1 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 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;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

1.1 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 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.

1.1 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.

1.1 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 условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

1.1 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 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.

1.1 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 АУ СОН ТО И ДПО «РСРЦН «Семья»;
- 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 также 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 также 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.