Утверждено
приказом директора
КОГОАУ «Гимназия г. Уржума»
от 15 сентября 2022 года № 121-о

Феофилатов Дмитрий Николаевич

Подписан: Феофилатов Дмитрий Николаевич
DN: C=RU, S=Кировская область, L=г. Уржум, T=Директор, O="КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ""ГИМНАЗИЯ Г. УРЖУМА""", СНИЛС=06446348978, ИНН=433400354673, E=urzhum_gimns@mail.ru, G=Дмитрий Николаевич, SN=Феофилатов, CN=Феофилатов Дмитрий Николаевич
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2023.09.15 16:08:51+03'00'
Foxit Reader Версия: 10.1.1

ПОРЯДОК
проведения периодических проверок (аудитов) в области обработки и обеспечения безопасности персональных данных в Кировском областном государственном общеобразовательном автономном учреждении «Гимназия г. Уржума»

Уржум, 2022

Содержание

1. Общие положения

1.1. Назначение

Настоящий Документ определяет порядок организации и проведения внутренних проверок (аудитов) процессов обработки персональных данных (далее – Порядок) в Кировском областном государственном общеобразовательном автономном учреждении «Гимназия г. Уржума» (далее – Организация).

1.2. Цель принятия документа

Настоящий Порядок принят в целях:

- обеспечения соответствия процессов обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- своевременного обнаружения несоответствий требованиям процесса обработки персональных данных и их устранения.

1.3. Область применения

Настоящий документ применяется:

- к процессам Организации, в которых ведется обработка персональных данных.
- ко всем обособленным подразделениям Организации;
- ко всем офисам и удаленным сотрудникам, независимо от их местоположения.

1.4. Аудитория

Порядок предназначен для следующих категорий сотрудников Организации и лиц:

- сотрудник, ответственный за организацию обработки персональных данных;
- сотрудники, в обязанности которых входит обработка персональных данных;
- руководители подразделений;
- сотрудники, в обязанности которых входит организация и обеспечение документооборота;
- подразделения, в обязанности которых входит разработка и поддержка сервисов и информационных систем персональных данных;
- лица, которым Организацией поручено обрабатывать персональные данные.

Под сотрудниками в настоящем положении понимаются лица, состоящие в трудовых или договорных отношениях с Организацией, а также сотрудники организаций, которым Организацией поручена обработка персональных данных (далее - “сотрудники”).

Перечисленные сотрудники перед предоставлением доступа к персональным данным должны быть ознакомлены с настоящим документом в соответствии с *Порядком предоставления доступа к персональным данным*.

1.5. Нормативные ссылки

Положение разработано в целях реализации следующих нормативно-правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.6. Срок действия и порядок внесения изменений

Порядок действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим.

Порядок подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, требований со стороны партнеров, изменения оценки рисков информационной безопасности. Изменения в документ вносятся путем издания новой версии и ознакомления с ним сотрудников, а также лиц, осуществляющих обработку персональных данных.

Срок хранения после прекращения действия: постоянно.

1.7. Используемые сокращения

СКЗИ – средства криптографической защиты информации.

2. Порядок проведения проверок

2.1. Общие сведения о внутренних проверках (аудитах)

2.1.1. Внутренние проверки (аудиты) проводятся с целью оценки соответствия требованиям процессов обработки персональных данных в Организации.

2.1.2. Внутренние проверки (аудиты) соответствия принимаемых мер по обеспечению безопасности персональных данных и установленного уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных, должны проводиться не реже 1 раза в 3 года. Для проведения таких проверок (аудитов) могут привлекаться на основании договора подрядные организации, имеющие лицензию Федеральной службы по техническому и экспортному контролю Российской Федерации на деятельность по технической защите конфиденциальной информации, а также, при необходимости, лицензию Федеральной службы безопасности Российской Федерации на деятельность, связанную со средствами шифрования.

2.1.3. Организация аудитов включает:

- Разработку программы внутренних проверок (аудитов);
- Разработку плана внутренних проверок (аудитов);
- Проведение внутренних проверок (аудитов);

2.1.4. Программа проверок (аудитов) – совокупность мероприятий по проведению одной или нескольких проверок (аудитов), запланированных на конкретный период времени и направленных на достижение конкретной цели – обеспечение соответствия процессов обработки персональных данных требованиям законодательства, нормативных документов и документов, принятых в Организации.

2.1.5. План проверки (аудита) - описание деятельности и мероприятий по проведению проверки (аудита).

2.2. Порядок формирования программы проверок (аудитов)

2.2.1. Программа проверок (аудитов) планируется сроком на 1 календарный год.

2.2.2. При проведении проверок (аудитов) необходимо учитывать степень доступности сотрудников, задействованных в их проведении.

2.2.3. В отсутствие ресурсов для выполнения программы проверок (аудитов) может быть приглашен внешний аудитор.

2.2.4. Программа проверок (аудитов) должна быть составлена таким образом, чтобы за проверяемый период были охвачены:

- все процессы обработки персональных данных;
- все подразделения;
- все географические расположения;
- все сервисы и информационные системы Организации.

2.2.5. Типовая форма программы внутренних проверок (аудитов) приведена в Приложении № 1.

2.3. План проверки (аудита)

2.3.1. План внутренней проверки (аудита) процессов обработки и обеспечения безопасности персональных данных формируется сотрудником, ответственным за проведение проверки (аудита) – внутренним аудитором и согласовывается с сотрудником, ответственным за организацию обработки персональных данных и сотрудником, ответственным за обеспечение безопасности персональных данных (информационной безопасности) в Организации.

2.3.2. Перечень и описание отдельных вариантов проверок, которые должны быть включены в план, приведен в разделе 3 Порядка.

2.3.3. План должен включать:

- направление проверки (персональные данные);
- должность и ФИО внутреннего (их) аудитора (ов);
- цель проверки (аудита);
- описание проверки;
- подразделения, входящие в проверку;
- критерии проверки (аудита) – требования, по которым будет проходить проверка;
- основные вопросы проверки (аудита);
- время проведения проверки (аудита);
- форма проведения (очная, заочная, по документам, с интервьюированием).

2.3.4. В зависимости от структуры подразделений, особенностей процессов и разграничения полномочий план проверки (аудита) может быть разработан специально под отдельное подразделение или процесс.

2.3.5. Для сервисов и информационных систем персональных данных план проверок формируется в рамках процессов информационных технологий и информационной безопасности.

2.4. Порядок оповещения работников о проведении проверки

2.4.1. Работники Организации должны быть оповещены о проведении проверки не позднее, чем за 5 рабочих дней до её начала. Оповещение должно содержать план проверки.

2.5. Отчет о результатах проверки (аудита)

2.5.1. По итогам проверки (аудита) внутренним аудитором формируется отчет, представляющий собой совокупность наблюдений о соответствии или несоответствии требованиям проверенных подразделений и процессов.

2.5.2. Наблюдения фиксируются в электронной таблице в виде записей, содержащих:

- направление проверки (персональные данные);
- название несоответствия;
- описание;
- подразделение;
- требование (пункт федерального закона, иного нормативного документа или локального акта);
- соответствие/несоответствие/рекомендация;
- сотрудник, выявивший несоответствие;
- сотрудник подразделения, ответственный за устранение несоответствия;
- срок устранения несоответствия;
- срок повторной проверки.

2.5.3. Таблица после составления распечатывается и подписывается аудитором.

2.5.4. Сотрудник, ответственный за организацию обработки персональных данных, обеспечивает ведение реестра несоответствий и нарушений, организовывает работу по их устранению, координирует и содействует работе ответственных за устранение несоответствий и нарушений.

2.5.5. При выявлении совокупности одинаковых несоответствий, либо в случае выявления отдельного практически-сложного случая, может потребоваться создание рабочей группы наблюдения или выделение дополнительных ресурсов. Такая группа наблюдений или кейс формируются в проект и выполняются в форме проекта, включая обоснование, формирование технического задания, выполнение работ, закупку, принятие в эксплуатацию. Лицами, обеспечивающими реализацию таких проектов в Организации, являются *сотрудник ответственный за организацию обработки персональных данных* и *сотрудник ответственный за безопасность персональных данных (информационную безопасность)*.

2.5.6. По результатам проведения внутренних проверок по итогам года сотрудник, ответственный за организацию обработки персональных данных формирует и представляет руководству Организации отчет.

3. Перечень проводимых проверок

3.1. Проверка соблюдения принципов обработки персональных данных

В ходе проверки соблюдения принципов обработки персональных данных осуществляются следующие мероприятия:

- проверка актуальности документов, определяющих политику Организации в отношении обработки персональных данных;
- проверка процессов обработки персональных данных на предмет обработки избыточных персональных данных, а также на предмет превышения установленных сроков хранения персональных данных;
- проверка обоснованности установленных целей обработки персональных данных.

3.2. Проверка правовых оснований для обработки персональных данных

В ходе проверки правовых оснований для обработки персональных данных осуществляются мероприятия:

- проверка договоров с субъектами персональных данных;
- проверка договоров с лицами, которым Организацией поручена обработка персональных данных;
- проверка договоров с лицами, которые поручают Организации обработка персональных данных;
- проверка наличия согласий в ситуациях, когда такое основание необходимо;
- проверка наличия согласий в письменной форме, если такие согласия необходимы;
- проверка наличия законных и иных оснований для обработки персональных данных;
- проверка сроков обработки персональных данных и наличия правовых оснований.

3.3. Проверка соблюдения Порядка предоставления доступа к обработке персональных данных

В ходе проверки соблюдения *Порядка предоставления допуска к персональным данным в Кировском областном государственном общеобразовательном автономном учреждении «Гимназия г. Уржума»* осуществляются следующие мероприятия:

- проверка актуальности документа *«Перечень должностей сотрудников, допущенных к обработке персональных данных в автоматизированной форме и без использования средств автоматизации»*;
- проверка наличия заполненных листов (журналов) ознакомления сотрудника под роспись с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных
- проверка ведения *журнала инструктажей по правилам обработки и обеспечения безопасности персональных данных*;
- проверка наличия подписанных *обязательств о неразглашении конфиденциальной информации*;
- проверка наличия заявок на предоставление (изменение/прекращение) доступа к информационным системам персональных данных;
- проверка наличия учетных записей пользователей;
- проверка соответствия прав доступа пользователей в информационных системах персональных данных ранее поданным заявкам на предоставление доступа.

3.4. Проверка соблюдения порядка взаимодействия с субъектами персональных данных

В ходе проверки соблюдения *Положения о порядке взаимодействия с субъектами персональных данных и их представителями по вопросам обработки персональных данных* осуществляются следующие мероприятия:

- проверка порядка принятия и обработки обращений и вопросов субъектов персональных данных;

- проверка времени реагирования на обращения субъектов персональных данных согласно требованиям ст.14, 20, 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- проверка факта размещения политики обработки персональных данных в открытом доступе;
- проверка ведения журнала учета обращений субъектов;
- проверка осведомленности работников о порядке взаимодействия с субъектами персональных данных, в том числе о правах субъектов персональных данных;
- проверка осведомленности сотрудников по вопросам разъяснения юридических последствий отказа субъекта в предоставлении персональных данных.

3.5. Проверка порядка обращения с машинными носителями персональных данных

В ходе проверки порядка обращения с машинными носителями персональных данных осуществляются следующие мероприятия:

- проверка ведения *Журнала учета съемных носителей*;
- проверка условий хранения съемных носителей, выданных работникам;
- проверка ведения *Журнала учета несъемных машинных носителей*;
- проверка порядка уничтожения машинных носителей персональных данных, в т.ч. наличие *Актов уничтожения*;
- проверка осведомленности работников о порядке использования съемных машинных носителей персональных данных.

3.6. Проверка соблюдения Порядка неавтоматизированной обработки персональных данных

В ходе проверки соблюдения *Инструкции по обработке персональных данных, осуществляемой без использования средств автоматизации* осуществляются следующие мероприятия:

- проверка актуальности и соблюдения сотрудниками документа *«Перечень мест хранения материальных носителей персональных данных*;
- проверка сохранности бумажных носителей персональных данных;
- проверка осведомленности работников о порядке неавтоматизированной обработки персональных данных;
- проверка избыточности хранения документов;
- проверка типовых форм документов, с использованием которых ведется сбор персональных данных;
- проверка актов уничтожения документов.

3.7. Проверка условий эксплуатации средств криптографической защиты информации

В ходе проверки условий эксплуатации средств криптографической защиты информации (далее – СКЗИ) осуществляются следующие мероприятия:

- проверка оснащения серверных помещений техническими устройствами, сигнализирующими о несанкционированном вскрытии (либо проверка опечатывания серверных помещений);
- проверка актуальности утвержденного перечня лиц, имеющих право доступа в серверные помещения;

- проверка назначения администратора СКЗИ, пользователей СКЗИ;
- проверка наличия и порядка хранения инструкции по эксплуатации СКЗИ, инструкции пользователя СКЗИ, дистрибутивов СКЗИ, формуляра СКЗИ;
- проверка соблюдения требований инструкции по эксплуатации СКЗИ, правил пользования СКЗИ.

Приложение № 1. Типовая форма программы внутренних проверок

Программа
внутренних проверок (аудитов) процессов обработки и обеспечения безопасности персональных данных

_____

(период)

Сроки проведения	Процесс	Наименование мероприятия	Ответственный за проведение
<Подразделение N>			
с (__.__.___) по (__.__.___)	Отдел М	Проверка соблюдения принципов обработки персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка соблюдения порядка предоставления доступа к обработке персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка правовых оснований для обработки персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка соблюдения порядка взаимодействия с субъектами персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка порядка обращения с машинными носителями персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка порядка эксплуатации персональных компьютеров при доступе к сервисам и информационным системам персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка соблюдения порядка неавтоматизированной обработки персональных данных	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка условий эксплуатации средств криптографической защиты информации	*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Подготовка ежегодного отчета по результатам внутренних проверок порядка обработки и обеспечения безопасности персональных данных	*(Фамилия И.О.)*