

10.5. План внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

(Выписка из Плана работы государственного бюджетного общеобразовательного учреждения
Ставропольского края «Гимназия № 25», утвержденного приказом государственного бюджетного
общеобразовательного учреждения Ставропольского края «Гимназия № 25» от 31.08.2023 г.
№439/2-ОД)

План внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных на 2023-2024 учебный год содержит перечень внутренних проверок, сроки их исполнения и исполнителей.

План распространяется на все информационные системы персональных данных гимназии.

№	Наименование мероприятия	Сроки исполнения/ Периодичность	Ответственные
1.	Контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка ПДн		
1.1	Проверка актуальности перечня должностных лиц, допущенных к работе с ПДн	Сентябрь 2023, февраль 2024	Комиссия по проведению внутреннего контроля (далее – Комиссия) /ответственный за обработку
1.2.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Декабрь 2023, июнь 2024	Руководители подразделений, администратор ИСПДн Грицак К.Г., Комиссия
1.3.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Декабрь 2023, июнь 2024	Руководители подразделений, ответственный за обработку ПДн, Комиссия
1.4	Проверка исполнения режима доступа в серверное помещение	Декабрь 2023, июнь 2024	Администратор ИСПДн Грицак К.Г., Комиссия
1.	Контроль доступа к приложениям информационных систем, в которых осуществляется обработка ПДн		
2.1.	Контроль использования предоставленных прав доступа (в том числе и право удаленного доступа)	Сентябрь 2023, март 2024	Администратор ИСПДн Грицак К.Г., Комиссия по контролю уровня защищенности информации в ИС
2.2.	Соответствие используемых пользователями ИСПДн полномочий параметрам (матрице) доступа	Ежегодно, сентябрь	Администратор ИСПДн, комиссия по персональным данным, Комиссия по контролю уровня защищенности информации в ИС
2. Контроль порядка обращения с носителями ПДн			
3.1.	Проверка корректности ведения журнала учета машинных носителей и соответствия записей в журнале записям в автоматизированной системе контроля съемных магнитных носителей информации	Ежеквартально	Администратор ИСПДн Грицак К.Г., Комиссия
3.2.	Своевременность проведения мероприятий по уничтожению персональных данных	Ежеквартально	Руководители подразделений, ответственный за обработку ПДн, комиссия по уничтожению персональных данных
3.3	Контроль правильности эксплуатации средств криптографической защиты информации	Сентябрь 2023, февраль 2024	Комиссия

№	Наименование мероприятия	Сроки исполнения/ Периодичность	Ответственные
3. Проверка выполнения запросов субъектов персональных данных			
4.1.	Контроль актуальности ведения журнала учета обращений субъектов ПДн по вопросам обработки их ПДн	Ежеквартально	Ответственный за обработку ПДн, Комиссия
4.2	Наличие необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн	Ежегодно сентябрь	Ответственный за обработку ПДн, Комиссия
4. Контроль выявления и нейтрализации нарушений режима обработки ПДн			
5.1	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ноябрь 2023, май 2024	Администратор ИСПДн Грицак К.Г., Комиссия
5.2	Выборочная проверка АРМ пользователей на предмет наличия возможных вредоносных программ и запрещенных информационных ресурсов	Ежеквартально	Администратор ИСПДн Грицак К.Г.
5.3.	Проведение аудита и регистрации событий безопасности в сегментах ГИС	По отдельному графику	Администратор ИСПДн Грицак К.Г.
5. Контроль соблюдения требований режима обработки ПДн			
6.1.	Соблюдение порядка работы со средствами <u>защиты информации</u>	Ежегодно	Администратор ИСПДн Грицак К.Г.,
6.2.	Соблюдение пользователями ИСПДн требований антивирусной защиты	Ежеквартально	Администратор ИСПДн Грицак К.Г.
6.3.	Соблюдение порядка резервирования баз данных, иной защищаемой информации и хранения резервных копий	Ежегодно	Администратор ИСПДн Грицак К.Г., Комиссия по контролю уровня защищенности информации в ИС
6.4.	Контроль за внесением изменений в программное обеспечение, за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Ноябрь – декабрь 2023	Руководители подразделений, администратор ИСПДн Грицак К.Г.
6.5.	Осуществление контроля выполнения требований о защите информации в сегментах ГИС (согласно инструкции)	Декабрь 2022, июнь 2023	Комиссия по контролю уровня защищенности информации в ИС
6. Контроль соблюдения пользователями ИСПДн парольной политики			
7.1.	Проверка сроков действия паролей	Октябрь	Администратор ИСПДн Грицак К.Г
7.2.	Проверка пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей	Ежеквартально	Администратор ИСПДн Грицак К.Г.
7. Анализ и пересмотр имеющихся угроз безопасности ПДн			
8.1.	Анализ и пересмотр имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	Комиссия по персональным данным, администратор ИСПДн Грицак К.Г.
8.2.	Корректировка Частных моделей угроз безопасности ПДн при их обработке в ИСПДн	Ежегодно	
8. Проверка корректности классификации ИСПДн			
9.1.	Проверка правильности определения категорий обрабатываемых в ИСПДн ПДн	Ежегодно	Комиссия по классификации информационных систем
9.2.	Корректировка объема обрабатываемых ПДн (количество субъектов ПДн, ПДн которых обрабатываются в ИСПДн)		
9.3.	Уточнение структуры ИСПДн		
9.4.	Анализ режимов обработки ПДн и разграничения прав доступа пользователей ИСПДн	Ежегодно	Администратор ИСПДн Грицак К.Г.

№	Наименование мероприятия	Сроки исполнения/ Периодичность	Ответственные
9.5.	Уточнение местонахождения технических средств ИСПДн	По необходимости	
9. Поддержание в актуальном состоянии нормативно-организационных документов по вопросам обеспечения безопасности ПДн			
10.1	Актуализация локальных нормативных актов по вопросам обеспечения безопасности ПДн	после каждого изменения законодательных и иных <u>нормативных правовых актов</u> по защите ПДн и отраслевых стандартов / по результатам проверки	Ответственный за обработку ПДн - информатизации Рыженко Т.А.
10.2	Проверка актуальности локальных нормативных актов по вопросам обеспечения безопасности ПДн	Октябрь 2023	Комиссия
10.2.	Проверка актуальности сведений, содержащихся в уведомлении Роскомнадзора об обработке (о намерении осуществлять обработку) персональных данных	Сентябрь 2023	Ответственный за обработку ПДн - зам. директора по информатизации Рыженко Т.А.
10. Обучение и проверка знаний работников по вопросам обеспечения безопасности ПДн			
11.1.	Контроль ознакомления вновь принимаемых работников с локальными нормативными актами, регламентирующими обработку ПДн	Октябрь 2023	Ответственный за обработку ПДн - зам. директора по информатизации Рыженко Т.А., Комиссия