ПЛАН МЕРОПРИЯТИЙ

**по обеспечению безопасности защищаемой информации,
выполнению требований законодательства по защите информации,
а также по контролю уровня защищенности и выполнения мер
по защите информации в сегменте АИС «Сетевой город. Образование»**

Разовые мероприятия

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
1.	Назначение ответственных за защиту информации в Гимназии № 2 (или: Создание подразделения по Гимназии № 2	Директор, 2018		
2.	Формирование комиссии по классификации сегмента ГИС «Контингент»	Директор, 2018		
3.	Анализ актуальных угроз безопасности информации в сегменте ГИС «Контингент» на основании документа «Модель угроз ГИС «Контингент», содержащего, в том числе модель нарушителя	Ответственный за организацию обработки персональных данных, 2018		
4.	Классификация сегмента ГИС «Контингент», разработка акта классификации	Комиссия по классификации, 2018		
5.	Формирование группы реагирования на инциденты информационной безопасности в Гимназии № 2	Директор, 2018		
6.	Разработка и утверждение инструкции по реагированию на инциденты информационной безопасности в Гимназии № 2	Администратор безопасности, директор, 2018		
7.	Разработка и утверждение правил использования средств криптографической защиты информации в Гимназии № 2	Администратор безопасности, директор, 2018		
8.	Разработка и утверждение инструкции пользователя сегмента ГИС «Контингент», содержащей: − общие обязанности пользователя по защите информации; − правила управления идентификаторами, учетными записями и паролями; − противодействие методам социальной инженерии и правила работы с электронной почтой;	Администратор безопасности, директор, 2018		

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
	− правила работы со съемными носителями информации.			
9.	Разработка и утверждение политики информационной безопасности в Гимназии № 2 содержащей: − перечень сведений конфиденциального характера, обрабатываемых в Гимназии № 2 − описание технологических процессов обработки защищаемой информации в информационных системах Гимназии № 2 − правила и процедуры идентификации и аутентификации пользователей информационных систем Гимназии № 2 − правила разграничения доступа к ресурсам информационных систем Гимназии № 2 − правила и процедуры управления информационными потоками; − правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения; − правила защиты машинных носителей информации, контроля интерфейсов ввода-вывода и гарантированного уничтожения информации; − правила взаимодействия информационных систем Гимназии № 2 с внешними информационными системами; − правила и процедуры выявления, анализа и устранения уязвимостей; − правила и процедуры контроля установки обновлений программного обеспечения; − правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации; − правила и процедуры резервирования технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций;	Администратор безопасности, директор, 2018		

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
	− ролевую систему доступа к ресурсам информационных систем Гимназии № 2 − перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами информационных систем Гимназии № 2; − перечень лиц, допущенных в помещения, в которых производится обработка конфиденциальной информации; − список разрешающих правил взаимодействия с внешними телекоммуникационными сетями; − список разрешенного программного обеспечения.			
10.	Формирование требований к системе защиты информации на основании документа «Техническое задание на создание системы защиты информации в АИС «Сетевой город. Образование»	Администратор безопасности, директор, 2023		
11.	Проектирование системы защиты информации	Администратор, директор, 2023		
12.	Организация контролируемой зоны и утверждение положения «О контролируемой зоне»	Администратор, директор, 2023		
13.	Закупка необходимы сертифицированных средств защиты информации	Директор, 2023		
14.	Реализация проекта системы защиты информации (установка и настройка средств защиты информации)	Администратор, 2023		
15.	Приемка системы защиты информации сегмента АИС «Сетевой город. Образование»	Администратор, директор, 2023		
16.	Ввод сегмента АИС «Сетевой город. Образование» в эксплуатацию на основании акта о приемке в постоянную эксплуатацию системы защиты информации сегмента ГИС «РО»	Директор, 2023		

Контролирующие и периодические мероприятия

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
Документирование					
1.	Контроль наличия согласий на обработку персональных данных субъектов персональных данных, чьи ПДн обрабатываются Гимназии № 2	Ответственный за организацию обработки ПДн	Вручную	Ежеквартально	
2.	Контроль наличия соглашений о неразглашении конфиденциальной информации, подписанных сотрудниками, допущенными к обработке такой информации	Ответственный за организацию обработки ПДн	Вручную	Ежеквартально	
3.	Контроль актуальности внутренней документации по защите информации, в том числе списков лиц, допущенных к обработке конфиденциальной информации	Ответственный за организацию обработки ПДн, Администратор безопасности	Вручную	Ежеквартально либо при существенном изменении законодательства в сфере защиты информации	
4.	Контроль наличия актуальных договоров с организациями, которым передаются персональные данные, а также наличия в этих договорах пунктов, регламентирующих обязанность этих организаций обеспечивать конфиденциальность персональных данных	Ответственный за организацию обработки ПДн	Вручную	Каждые полгода	
5.	Пересмотр актуальных угроз безопасности и актуализация	Администратор безопасности	Вручную	Ежегодно, либо при изменении нормативной	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	документа «Модель угроз безопасности информации»			документации в сфере моделирования угроз безопасности информации, либо при поступлении информации о новых угрозах, актуальных для информационных систем Гимназии № 2	
6.	Ежегодный контроль сегмента АИС «Сетевой город. Образование»	Организация-лицензиат ФСТЭК России, привлекаемая для проведения аттестационных испытаний	Согласовываются в документе «Программа и методики аттестационных испытаний»	1 раз в год, либо при существенном изменении структурно-функциональных характеристик сегмента ГИС «РО»	
Информирование и обучение персонала					
7.	Доведение до персонала информации о новых угрозах информационной безопасности	Администратор безопасности	Устные лекции, информирование по каналам электронной почты	Не реже 1 раза в месяц	
8.	Доведение до персонала положений законодательства в сфере защиты персональных данных	Ответственный за организацию обработки ПДн	Устные лекции, информирование по каналам электронной почты	Не реже 1 раза в квартал	
9.	Доведение до персонала положений внутренних нормативных документов по защите информации	Администратор безопасности, Ответственный за организацию	Устно	По мере появления новых внутренних документов или по мере существенного изменения старых	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
		обработки ПДн			
10.	Повышение квалификации и переподготовка лиц, ответственных за защиту информации Гимназии № 2 на курсах по направлению «Информационная безопасность» (не менее 72 часов)	директор	Планирование учебных курсов	Не реже 1 раза в 5 лет	Учебные курсы должны быть согласованы со ФСТЭК России
11.	Проверка осведомленности персонала в сфере защиты информации	Администратор безопасности, Ответственный за организацию обработки ПДн	Устный опрос, письменное тестирование, имитация действий злоумышленника	Ежеквартально	
Физический контроль					
12.	Выборочный осмотр рабочих мест пользователей на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения неучтенных технических средств	Администратор безопасности	Визуальный осмотр	Ежедневно	
13.	Заведение, удаление учетных записей пользователей. Наделение, лишение, изменение полномочий пользователей по доступу к ресурсам сегмента АИС «Сетевой город. Образование»	Администратор безопасности	Secret Net Studio 8	По мере поступления заявок на заведение/удаление учетных записей и наделение/изменение полномочий в системе	
14.	Мониторинг учетных записей на	Администратор	Secret Net Studio 8	Еженедельно	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	предмет выявления неблокированных временных учетных записей или учетных записей уволенных сотрудников	безопасности			
15.	Смена собственного пароля и мониторинг своевременной смены паролей других привилегированных пользователей	Администратор безопасности	Secret Net Studio 8	Каждые 90 суток	
16.	Мониторинг своевременной смены паролей пользователями сегмента АИС «Сетевой город. Образование»	Администратор безопасности	Secret Net Studio 8	Ежедневно	
17.	Смена паролей доступа к интерфейсам управления сетевыми устройствами (коммутаторами, маршрутизаторами)	Администратор безопасности	Вручную	Каждые 90 суток	