Муниципальное бюджетное общеобразовательное учреждение
Лицей города Бирска муниципального района Бирский район
Республики Башкортостан

СОГЛАСОВАНО
Председатель первичной
профсоюзной организации
МБОУ Лицей г.Бирска
_____ Валиахметова Г.Г.
Протокол № 6 от 09.08.2024г.

УТВЕРЖДАЮ
Директор МБОУ Лицей г.Бирска
_____ М.А. Васенкова
Приказ № 24-К от 14.08.2024г.

ПЕРЕЧЕНЬ
мероприятий по защите информации в информационных системах в МБОУ Лицей г. Бирска

План мероприятий по защите информации в информационных системах МБОУ Лицей г. Бирска разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
1.	**Формирование требований к защите информации, содержащей**		
1.1.	Принятие решенияо необходимости защиты информации, содержащейся в ИС	-	-
1.2.	Классификация ИС по требованиям Защиты информации определение уровня защищенности персональных данных (далее– ПДн) при их обработке в ИС	Перед созданием системы защитыипри необходимостивходе эксплуатации ИС	Определение класса защищенности ИС и уровн Осуществляется при создании ИС, а также вход или технических особенностей ее построения (и т.д.).
1.3.	Определение угроз безопасности информации, реализация которых Может привести к нарушению безопасности информации в ИС, и разработка на их основе модели Угроз безопасности информации	Перед созданием системы защитыив ходе эксплуатации ИС при выявлении новых уязвимостей	Разрабатывается/ уточняется Модель угроз бе информации.
1.4.	Определение требований к системе Защиты информации ИС	Перед созданием системы защиты	Разрабатывается техническое задание на создан
2.	**Разработка системы защиты информации ИС**		
2.1.	Проектирование системы защиты информации ИС	Довводав эксплуатацию при необходимости	Разработка Проекта на систему защиты. Выбор Класса защищенности ИС, уровня защищенно информации ,включенных в Модель угро
2.2.	Разработка эксплуатационной		

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
3.			Возникновению угроз безопасности информации
		Внедрение системы защиты информации ИС	
3.1.	Установкаи настройкасредств Защиты информации в ИС	Довводав эксплуатацию при необходимости	Установка и настройка средств защиты инфо документацией на систему защиты информации информации.
3.2.	Разработкадокументов, Определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИС входе ее эксплуатации	Довводав эксплуатацию при необходимости	Разработка организационно-распорядительных д
3.3.	Внедрение организационных мер Защиты информации	Довводав эксплуатацию при необходимости	Реализация правил разграничения доступа, регл Объектам доступа, и введение ограничений условий эксплуатации, состава и конфигураци Проверка полноты и детальности описания защите информации действий пользователей а мер защиты информации; Отработка действий должностных лиц и подра информации.
3.4.	Предварительные испытания системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка работоспособности системы защиты и возможности опытной эксплуатации системы за

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
3.8.	Аттестация ИС по требованиям Защиты информации и вводее в действие	До вводав эксплуатациои при необходимости	Проводится совместно с лицензиатами ФСТЭК
4.	**Обеспечение защиты информации в ходе эксплуатации аттестова**		
4.1.	Планирование мероприятий по защите информации в ИС	Вместе с вводом ИС в эксплуатацию	Разработка, утверждение и актуализация плана
4.2.	Анализ угроз безопасности информации в ИС	Не реже одного раза в квартал; При внедрении новых узлови/или технологий вИС; При появлении информационных уязвимостях	Входе анализа угроз безопасности информации выявление, анализ и устранение уязвимостей Ин анализ изменения угроз безопасности информа оценка возможных последствий реализации уг
4.3.	Управление (администрирование) системой защитыинформации ИС	Постоянно входе эксплуатации ИС	Входе управления (администрирования) систем Управление учетными записями пользовател разграничения доступа в ИС; Управление средствами защиты информаци программно-аппаратных средств ,в том числе функционирования ИС; мониторинги анализ события безопасности заре обеспечение функционирования системы защ

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
4.5.	Выявление инцидентов и реагирование на них	Постоянно входе эксплуатации ИС; Не реже одного раза в год проведение внутреннего аудита информационной безопасности	Входе реагирования на инциденты осуществляю Обнаружение идентификация инцидентов, в том в работе технических средств, программного обе правил разграничения доступа, неправомерн вредоносных компьютерных программ (вирусо инцидентов; своевременное информирование пользователями за выявление инцидентов и реагирование на и системе; анализ инцидентов, в том числе определение исто оценка их последствий; планирование и принятие мер по устранению и сегментов в случае отказа в обслуживании или правил разграничения доступа, неправомерн вредоносных компьютерных программ (вирусо инцидентов.
4.6.	Информирование и обучение Персонала ИС	Не реже одного раза в Два года	Входе информирования и обучения персонала ИС Информирование персонала ИС о появлении акт безопасной эксплуатации ИС; доведение до персонала ИС требований по защи распорядительных документов по защите инф обучение персонала ИС правилам эксплуатации проведение практических занятий, тренир

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			Информации , содержащейся в ИС; Принятие решения по результатам контроля за содержащейся в ИС, о необходимости доработ Контроль за обеспечением уровня защищенно самостоятельно и (или) с привлечением орган технической защите конфиденциальной инфор
5.	**Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия**		
5.1.	Архивирование информации, Содержащейся в ИС	При выводе из эксплуатации аттестованной ИС или после принятия	Архивирование информации, содержащейся в И дальнейшего использования.