Согласовано
Председатель Первичной
Профсоюзной организации
МОБУ гимназия №1
г.Благовещенска
_____/Гайнетдинова Л.Д./
Протокол №___
от «___» _____2025 г.

Утверждаю
Директор МОБУ
гимназия №1 г.Благовещенска
_____/Жилина Н.С./
Приказ № ____
от «___» _____2025 г.

П л а н
мероприятий по защите информации в информационных системах МОБУ гимназия №1 г. Благовещенска

План мероприятий по защите информации в информационных системах МОБУ гимназия №1 г. Благовещенска разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

№№	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
	1. Формирование требований к защите информации, содержащейся в ИС		
1.1.	Принятие решения о необходимости защиты информации, содержащейся в ИС	Перед созданием системы защиты	Формирование требований к защите информации, содержащейся в ИС
1.2.	Классификация ИС по требованиям Защиты информации, определение уровня защищенности персональных данных (далее – ПДн) при их обработке в ИС	При необходисомти входа, или эксплуатации ИС	Определение класса защищенности ИС и уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, а также в ходе эксплуатации при изменении состава, структуры, или технических особенностей построения ИС (при изменении программного обеспечения, технологии использования и т.д.)
1.3.	Определение угроз безопасности информации, реализация которых может приести к нарушению безопасности информации в ИС и разработка на их основе модели угроз безопасности	Перед созданием системы защиты в ходе эксплуатации ИС при выявлении новых уязвимостей.	Разрабатывается/ уточняется модель угроз безопасности и модель нарушения безопности информации.
1.4.	Определение требований к системе защиты информации	Перед созданием системы защиты	Разрабатывается техническое задание на создание системы защиты информации ИС
	2. Разработака системы защиты информации ИС		
2.1.	Проектирование системы защиты		Разработка проекта на систему защиты. Выбор мер по защите информации проводится исходя из класса защищенности ИС, уровня защищенности ПДн при необходимости их обработки в ИС и угроз безопсности информации, включенных в модель угроз безопасности, а также с учетом структурно – функциональных характеристик ИС. Определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.
2.2.	Разработка эксплуатационной документации на систему защиты информации ИС	До ввода в эксплуатацию при необходимости	Определяется структура ситемы защиты инфйормацииИС, включая соств (качество) и места размещения ее элментов. Осуществляется выбор средств защиты информации, сертифицированных на соотвествие требованиям по безопасности информации с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функциями безопасности этих средств и особенностями их реализации, а так же класса защищенности ИС и уровня защищенности ПДн при их обработке в ИС. Определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а так же устрнение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации.
	3. Внедрение системы защиты информации		
3.1.	Установка и настройка средств защиты информации в ИС	До ввода в эксплуатацию при необходимости	Установка и настройкм средств защиты информации в соответствие с эксплуатационной документацией на систему защиты информации ИС и документацией на средства защиты информации

3.2.	Разработка документоа, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИС в ходе ее эксплуатации		Разработака организационно – распорядительных документов по защите информации.
3.3.	Внедрение организационных мер защиты информации		Реализация правил разграничения доступа, регоаментирующих права доступа субъктов к объектам доступа, и введение ограничений на действия пользователей, а так же на изменения условий эксплуатации, состава и конфигурации технических средстви программного обеспечения. Проверка полноты и детальности описанияв организационно – распорядительных документахпо защите информации, действий пользователей – администраторов ИС по реализации организационных мер защиты информации. Отработка действий должностных лиц и подразделений, ответственных за реализациюмер защиты информации
3.4.	Предварительные испытания системы защиты информации ИС		Проверка работоспособности системы защиты информации ИС, а также принятие решения о возможности опытной эксплуатации системы защиты информации ИС.
3.5.	Опфтная эксплуатация системы защиты информации ИС		Проверка функционирования системы защиты информации ИС, в том числе реализованных мер защиты информации, а так же готовность пользователей и администраторов к эксплуатации системы защиты информации ИС.
3.6.	Анализ уязвимостей ИС и принятие мер защиты информации по их устранению.		Проведение анализа уязвимостей средств защиты информации, технических средств и программообеспечения ИС. Уточнение модели угроз безопасности информации и при необходимости, принятие дополнительных мер защиты информации, в случае выявления уязвимостей ИС, приводящих к возникновению дополнительных угроз безопасности информации.
3.7.	Приемочные испытания системы защиты информации ИС		Проверка выполнения требований к систе:ме защиты информации ИС в соответствие с техническим заданием на создание системы защиты информации ИС.
3.8.	Аттестация ИС по требованиям защиты информации и вводе в днйствие.		Проводится совмечтно с лицензиатами ФСТЭК России.
4. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС.			
4.1.	Планирование мероприятий по защите информации в ИС	Вместе с вводом ИС в эксплуатацию.	Разработка, утверждение и актуализация плана мероприятий по защите информации ИС.
4.2.	Анализ угроз безопасности информации	; Не реже одного раза в квартал; при внедрении новых узлов/или технологий в ИС; при появлении информационных уязвимостей.	В ходе анализа угроз безопасности информации в ИС, в ходе ее эксплуатации осуществлется выявление,анализ и устранение уязвимостей ИС; Анализ изменения угроз безопасности информации в ИС; Оценка возможных последствий реализации угроз безопасности информации в ИС.
4.3.	Управление (администрирование) системой защиты информации ИС	Постоянно в ходе эксплуатации ИС	В ходе управления (администрирования) системой защиты информации ИС осуществляются: - Управление учертными записями пользователей и поддержания в актуальном состоянии правил разграничения доступа в ИС; - Управление средствами защиты информаци ИС; управление обновлениями

			программ и программно – аппаратных ср5едств, в том числе средств защиты информации, с учетом особенностей фукнкционирования ИС; - Мониторинги анализа событий безопасности, зарегистрированных в ИС; - Обеспечение защиты функционирования системы безопаности информации, информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно – распорядитебльных документов по защите информации.
4.4.	Управление конфигурацией аттестованной ИС и ее системой защиты информации		В ходе управления конфигурацией ИС и ее системы защиты информации осуществляются: - Определение компонентов ИС и ее системы защиты информации подлежат изменениям в рамках управления конфигурацией; - Управления ищменениями ИС и ее системы защиты информации: разработка параметров настройки обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение з0ащиты информации, санкуионирование внесения изменений в ИС и ее систему защиты информации, документирование дбействий по внесению изменений в ИС и сохранение данных об изменениях конфигурации; - Контроль действий по внесению изменений в ИС и ее систему защиты информации.
4.5.	Выявление инцидентов и реагирование на них	Постоянно в ходе эксплуатации ИС; не реже одного раза в год проведение внутреннего аудита информационной безопасности	В ходе реагирования на инциденты осуществляется: - Обнаружение и идентификациф инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защит информации, нарушение правил рагранічения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов; - -своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе; - Анализ инцидентов, в том числе определение истояников и причин возникновения инцидентов, а так же оценка их последствий; - Плвнирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегменов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерныхдействий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.
4.5.	Информирование и обучение персонала ИС.	Не реже одного раза в два года	В зоде информирования и обучения персонала ИС осуществляются: -информирование персрнала о появление актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС; - доведение до персонала ИС требований по защите информации, а также положений оргнизационно – распорядительных документов по защите

			информации с учетом внесенных в них изменений; - обучение персонала ИС правилам эксплуатации отдельных средств защиты информации; - проведение практических занятий, тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты; - корнтроль осведомленности персонала ИС об угрозах безопасности информации уровня знаний персонала по вопросам обеспечния защиты информации.
4.7.	Контроль за обеспечением уровня защищенности нформации, содержащейся в ИС		В ходе контроля за обеспечением уровн защишщенности информации, содержащейся в ИС, осуществляется: - Контроль (анализ) защенности информации с учетом особенностей функционирования ИС; - - анализ и оценка ИС и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков системы защиты информации ИС; - - документирование процедур и результатов контроля за обеспечнбием уровня защищенности информации, содержащейся в ИС; - - Принятие решения по результатам контроля за обеспечением уровня защищенности иняормации, содержащейся в ИС, о небходимости доработки (модернизации) ее ситемы цровня защищенности информации; - - Контроль за обеспечением уровня защищенности информации, содержащейся в ИС, проводится самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельнось по технической защите конфидециальной информации.
5. Обеспечнение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.			
5.1.	Архивирование информации, содержащейся в ИС.	При выходе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации	Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости ее дальнейшего использования.
5.2.	Уничтожение (стирание) данных и остаточной информации с машинных носителей носителей информации и (или) уничтожение машинных носитиелей информации.		Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС. Про выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, производится физическое уничтожение этих машинных носителей информации.