Утверждено:
Заведующий
_____ Н.Г. Кадочникова
Приказ № 214 от 20.05.2021г.

Инструкция
по порядку контроля за обеспечением уровня защищенности информации в информационных системах

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

1. Обеспечение защиты информации в ходе эксплуатации информационной системы должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать следующие мероприятия:
планирование мероприятий по защите информации в информационной системе;
анализ угроз безопасности информации в информационной системе;
управление (администрирование) системой защиты информации информационной системы;
управление конфигурацией информационной системы и ее системой защиты информации;
реагирование на инциденты;
информирование и обучение персонала информационной системы;
контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе.
1.1. В ходе планирования мероприятий по защите информации в информационной системе осуществляются:
определение лиц, ответственных за планирование и контроль мероприятий по защите информации в информационной системе;
определение лиц, ответственных за выявление инцидентов и реагирование на них;
разработка, утверждение и актуализация плана мероприятий по защите информации в информационной системе;
определение порядка контроля выполнения мероприятий по обеспечению защиты информации в информационной системе, предусмотренных утвержденным планом.
План мероприятий по защите информации в информационной системе утверждается вместе с правовым актом органа исполнительной власти о вводе информационной системы в эксплуатацию.
Контроль выполнения мероприятий, предусмотренных планом мероприятий по защите информации в информационной системе, осуществляется в сроки, определенные указанным планом.
1.2. В ходе анализа угроз безопасности информации в информационной системе в ходе ее эксплуатации осуществляются:
выявление, анализ и устранение уязвимостей информационной системы;
анализ изменения угроз безопасности информации в информационной системе;
оценка возможных последствий реализации угроз безопасности информации в информационной системе.
Периодичность проведения указанных работ определяется оператором в организационно-распорядительных документах по защите информации.
1.3. В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:
определение лиц, ответственных за управление (администрирование) системой защиты информации информационной системы;
управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в информационной системе;
управление средствами защиты информации информационной системы;

управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования информационной системы;
централизованное управление системой защиты информации информационной системы (при необходимости);
мониторинг и анализ зарегистрированных событий в информационной системе, связанных с обеспечением безопасности (далее - события безопасности);
обеспечение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.
1.4. В ходе управления конфигурацией информационной системы и ее системы защиты информации осуществляются:
определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий;
определение компонентов информационной системы и ее системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;
управление изменениями информационной системы и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в информационную систему и ее систему защиты информации, документирование действий по внесению изменений в информационную систему и сохранение данных об изменениях конфигурации;
контроль действий по внесению изменений в информационную систему и ее систему защиты информации.
Реализованные процессы управления изменениями информационной системы и ее системы защиты информации должны включать процессы гарантийного и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, информационной системы.
1.5. В ходе реагирования на инциденты осуществляются:
обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения 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 источников и причин возникновения инцидентов, а также оценка их последствий;
планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

1.6. В ходе информирования и обучения персонала информационной системы осуществляются:

информирование персонала информационной системы о появлении актуальных угрозах безопасности информации, о правилах безопасной эксплуатации информационной системы;

доведение до персонала информационной системы требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

обучение персонала информационной системы правилам эксплуатации отдельных средств защиты информации;

проведение практических занятий и тренировок с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты;

контроль осведомленности персонала информационной системы об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

Периодичность проведения практических занятий и тренировок с персоналом, мероприятий по обучению персонала и контролю осведомленности персонала устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в два года.

1.7. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

контроль (анализ) защищенности информации с учетом особенностей функционирования информационной системы;

анализ и оценка функционирования информационной системы и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации информационной системы;

документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе;

принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, о необходимости доработки (модернизации) ее системы защиты информации.

Контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе, проводится оператором самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе 1 класса защищенности, устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в год.

Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в информационных системах 2 и 3 классов защищенности, устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационных систем, но не реже 1 раза в два года.

Утверждено:
Заведующий
_____ Н.Г. Кадочникова
Приказ № 214 от 20.05.2021г.

Состав комиссии по защите информации

Председатель комиссии	Кадочникова Н.Г., заведующий МБДОУ «Детский сад №27 «Семицветик» г.Юрги»
Члены комиссии	Матрошилова О.Н., заместитель заведующего по БОП МБДОУ «Детский сад №27 «Семицветик» г.Юрги»
	Коржуева Н.Б., главный бухгалтер МБДОУ «Детский сад №27 «Семицветик» г.Юрги»
	Рослова Т.Ю., старший воспитатель МБДОУ «Детский сад №27 «Семицветик» г.Юрги»
	Видус Т.П., специалист по кадрам МБДОУ «Детский сад №27 «Семицветик» г.Юрги»