

2.1.5. Мониторинг и анализ зарегистрированных событий в информационной системе, связанных с обеспечением безопасности информации;

2.1.6. Обеспечение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

2.2. Ответственный обязан:

2.2.1. Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации;

2.2.2. Знать состав, структуру, назначение и выполняемые задачи информационной системы, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку защищаемой информации;

2.2.3. Знать состав, структуру н назначение системы зашиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

2.2.4. В рамках обеспечения функционирования системы защиты информации информационной системы в ходе ее эксплуатации обеспечивать:

* исполнение требований по защите информации в соответствии с проектной и организационной-распорядительной документацией на систему защиты информации информационной системы;
* реализацию принятых решений по обеспечению защиты информации, обрабатываемой в информационной системе;
* информирование Ответственного за защиту информации о выявленных недостатках по результатам выполнения контрольных мероприятий;
* контроль работ, проводимых сторонними организациями на технических средствах информационной системы;
* неразглашение информации ограниченного доступа, ставшей доступной в ходе исполнения должностных обязанностей;

2.2.5. В рамках реализации функции управления учетными записями пользователей и поддержания в актуальном состоянии правил разграничения доступа в информационной системе, обеспечивать:

* верификацию (проверку), личности пользователя, его должностных (функциональных) обязанностей при заведении учетной записи пользователя;
* заведение, активацию, блокирование и уничтожение учетных записей пользователей в соответствии с установленным в ведомстве Регламентом управления доступом;
* пересмотр и при необходимости, корректировку учетных записей пользователей в соответствии с установленным в Школе Регламентом управления доступом;
* своевременное уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
* реализацию правил разграничения доступа и полномочий пользователей в информационной системе на основе утвержденной директором Школы системы разграничения доступа;
* контроль правил генерации и смены паролей пользователями информационной системы, реализации правил разграничения доступом, полномочий пользователей в информационной системе;
* устранение нарушений, связанных с генерацией и сменой паролей пользователями, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступа, установлением полномочий пользователей;

2.2.6. В рамках реализации функций управления средствами зашиты информации информационной системы обеспечивать:

* корректную эксплуатацию пользователями средств защиты информации;
* консультирование пользователей, участвующих в процессах обработки и обеспечения безопасности информации, по вопросам использования средств зашиты информации;
* техническое обслуживание средств защиты информации информационной системы в соответствии с эксплуатационной документацией на средства защиты информации;
* устранение выявленных в средствах защиты информации уязвимостей, в том числе путем установки обновлений программного обеспечения средств зашиты информации;
* периодический консоль работоспособности (неотключения) средств защиты информации;
* периодический контроль целостности программного обеспечения средств зашиты информации;
* периодический контроль соответствия настроек средств защиты информации;
* принятие мер по восстановлению работоспособности (правильности функционирования) и параметров настройки средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов, в случае выявления фактов нарушения работоспособности или отклонения параметров настроек средства защиты информации:
* периодический контроль соответствия состава средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер. направленных на устранение выявленных недостатков;
* периодическое выполнение тестирования функций безопасности средств зашиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств (для информационной системы с установленным классом защищенности 1 и 2);
* периодический контроль состава средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер. направленных на устранение выявленных недостатков;
* периодический контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер. направленных на устранение выявленных недостатков;
* исключение из состава информационной системы несанкционированно установленных средств защиты информации;
* восстановление несанкционированно удаленных средств защиты информации;
* настройку средств зашиты информации, направленных на устранение возможности использования выявленных уязвимостей (при необходимости);
* согласование изменения конфигурации системы защиты информации и настроек средств защиты информации с Ответственным за защиту информации;

2.2.7. В рамках реализации функций управления обновлениями программных н программно-аппаратных средств, в том числе средств защиты информации, обеспечивать:

* получение из доверенных источников и установку обновлений программного обеспечения, включая программное обеспечение средств зашиты информации;
* контроль целостности файлов обновлений;
* проверку соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств зашиты информации, установленного в информационной системе и выпущенного разработчиком;
* запись об установке (применении) обновлений в соответствующей эксплуатационной документации:
* обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной зашиты;
* обновление базы решающих правил систем обнаружения вторжений, применяемых в информационной системе (при наличии таковых);
* выполнение обновления программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств с целью устранения выявленных уязвимостей;

2.2.8. В рамках реализации функций централизованного управления системой защиты информации информационной системы обеспечивать:

* централизованное управление установкой, удалением, обновлением, конфигурированием и (или) контролем актуальности версий программного обеспечения средств защиты информации, эксплуатируемых в информационной системе;

2.2.9. В рамках реализации функций мониторинга и анализа зарегистрированных событий в информационной системе, связанных с обеспечением безопасности, обеспечивать:

* регистрацию событий безопасности в соответствии с перечнем событий, подлежащим регистрации в информационной системе;
* периодический просмотр журналов регистрации событий безопасности;
* реагирование на сбои при регистрации событий безопасности:
* оперативное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о попытках и (или) фактах несанкционированного доступа или подозрительных событиях;
* содействие при проведении расследований инцидентов информационной безопасности.

**3. ПРАВА ОТВЕТСТВЕННОГО ЗА УПРАВЛЕНИЕ (АДМИНИСТРИРОВАНИЕ) СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ**

3.1. Ответственный имеет право:

3.1.1. Знакомиться с локальными актами Школы, регламентирующую процессы обработки защищаемой информации:

3.1.2. Вносить предложения Ответственному за защиту информации по совершенствованию существующей системы защиты информации:

3.1.3. Требовать от пользователей информационных систем соблюдения требований Инструкции пользователя информационных систем Школы, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации;

3.1.4. Требовать от Ответственного за защиту информации оказания содействия в исполнении функций и обязанностей, предусмотренных настоящей Инструкцией;

3.1.5. Участвовать в расследовании инцидентов информационной безопасности и получать информацию об инцидентах информационной безопасности с целью совершенствования системы защиты информации информационной системы;

3.1.6. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность информации, вносить свои предложения по совершенствованию организационных н технических мер обеспечения безопасности информации;

3.1.7. Требовать прекращения работы в информационной системе, как в целом, так и отдельных пользователей информационной системы, в случае выявления нарушений требований по обеспечению безопасности информации или в связи с нарушением функционирования информационной системы;

3.1.8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности информации к Ответственному за защиту информации.

**4. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЗА УПРАВЛЕНИЕ (АДМИНИСТРИРОВАНИЕ) СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ**

4.1. Ответственный несет персональную ответственность:

4.1.1. За работоспособность н надлежащее функционирование системы защиты информации;

4.1.2. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией;

4.1.3. За разглашение информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

4.1.4. За несоблюдение требований локальных актов Школы, устанавливающих порядок работы с защищаемой информацией, не содержащей сведения, составляющую государственную тайну, в пределах, установленных трудовым договором (служебным контрактом).

**ЛИСТ ОЗНАКОМЛЕНИЯ**

**с Инструкцией ответственного за управление (администрирование)**

**системой зашиты информации информационных систем**

**МБОУ «Апастовская СОШ»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |