Приложение № 4

**ИНСТРУКЦИЯ**

**ПО УПРАВЛЕНИЮ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**2020 г.**

1. **Введение**
	1. Настоящая инструкция предназначена для обеспечения защиты информации, содержащейся в ИСПДн, в том числе персональных данных (далее ПДн), при работе с событиями информационной безопасности.
	2. Настоящая инструкция определяет:
		1. перечень событий безопасности в ИСПДн, подлежащих регистрации и сроки их хранения;
		2. состав и содержание информации о событиях безопасности, подлежащих регистрации;
		3. порядок сбора, записи и хранения информации о событиях безопасности в течение определенного времени хранения;
		4. порядок анализа зарегистрированных событий безопасности;
		5. порядок защиты информации о событиях безопасности.
2. **Перечень событий информационной безопасности ИСПДн, подлежащих регистрации**
	1. Перечень событий информационной безопасности ИСПДн, подлежащих регистрации, составляет администратор безопасности и утверждает ответственный за защиту информации.
	2. В перечень событий информационной безопасности ИСПДн должны быть включены события безопасности, имеющие отношение к возможности реализации угроз безопасности информации, обрабатываемой в ИСПДн, описанных в модели угроз безопасности информации.
	3. В перечень событий безопасности ИСПДн должны быть включены события безопасности, регистрируемые в журналах операционной системы технических средств ИСПДн и средств защиты информации (далее – СЗИ), а также события, связанные с информационной безопасностью в инфраструктуре ИСПДн.
3. **Состав и содержание информации о событиях информационной безопасности**
	1. Состав и содержание информации о событиях безопасности ИСПДн, подлежащих регистрации, составляет администратор безопасности и утверждает ответственный за защиту информации.
	2. Состав и содержание информации по каждому событию, включенному в список регистрации должны идентифицировать источник, время и результат события (Форма 1).
4. **Порядок сбора, записи и хранения информации о событиях безопасности.**
	1. Настройку журналов регистрации событий информационной безопасности в программном обеспечении ИСПДн и СЗИ осуществляет администратор системный ИСПДн на основании предоставленных полномочий и администратор безопасности каждый в своей части. Настройка осуществляется на основе утвержденного перечня событий безопасности, подлежащих регистрации и перечня состава и содержания информации о событиях безопасности в соответствии с эксплуатационной документацией на программно-технические средства ИСПДн.
	2. Администраторы системные ИСПДн и администратор безопасности должны не реже 1 раза в неделю просматривать журналы регистрации событий безопасности.
	3. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИСПДн и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца.
	4. Информация о событиях безопасности в ИСПДн, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности при ее обнаружении в журнале организационных событий безопасности (Форма 2).
5. **Порядок анализа зарегистрированных событий безопасности**
	1. При просмотре и сохранении журналов регистрации событий безопасности и при регистрации организационных событий информационной безопасности администратор безопасности должен анализировать события на наличие инцидентов. При подозрении на инцидент администратор безопасности действует в соответствии с разделом 2 «Положения по защите информации».
	2. Администратор безопасности должен подробно исследовать наиболее часто повторяющиеся события безопасности, выяснить причины их возникновения и устранить эти причины.
	3. На основании регистрируемой и сохраняемой информации о событиях информационной безопасности в ИСПДн администратор безопасности один раз в 3 месяца (квартал) составляет отчет о событиях безопасности по форме документа «Форма 3» и передает его ответственному за защиту информации для анализа защищенности ИСПДн.
6. **Порядок защиты информации о событиях безопасности.**
	1. Права доступа к файлам отчетов журналов безопасности и настройкам журналов установлены администратору безопасности и администраторам системным ИСПДн и отражены в матрице доступа.
	2. На информацию о событиях информационной безопасности распространяются все требования к защите информации в соответствии с «Положением по защите информации».
7. **Заключительные положения.**
	1. Администратор безопасности и администраторы системные ИСПДн должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.
	2. Администратор безопасности и администраторы системные ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы в ИСПДн под роспись. Обязанность ознакомления администратора безопасности и администраторов системных ИСПДн с настоящей инструкцией лежит на ответственном за защиту информации.

|  |  |  |
| --- | --- | --- |
| **Начальник управления информатизации и коммуникаций** |  | **И.Н. Гвоздевский** |

**Форма 1**

**Журнал
регистрации инцидентов при эксплуатации ИСПДн**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Краткое описание инцидента | Категория инцидента | Дата | Подпись | Отметка об устранении последствий инцидента |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Форма 2**

**Журнал
учета организационных событий безопасности**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование события | Описание события | Дата | Подпись |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Форма 3**

**Отчет о событиях безопасности за период с \_\_\_\_\_\_ 20\_\_ г. по \_\_\_\_\_\_\_ 20\_\_ г., зарегистрированных в ИСПДн**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование события | Источник (причина) | Дата | Примечание |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |