СОГЛАСОВАНО
Начальника Управления
защиты информации и специальной
документальной связи Аппарата
Губернатора Ханты-Мансийского
автономного округа – Югры

_____ А.Ю.Чиликов

ноября 2016г.

УТВЕРЖДАЮ
Заместитель Руководителя
Аппарата Губернатора
Ханты-Мансийского
автономного округа – Югры

_____ М.А.Киселев

ноября 2016г.

ПОЛОЖЕНИЕ
о порядке выявления и реагирования на инциденты информационной безопасности в Аппарате Губернатора Ханты-Мансийского автономного округа – Югры

СОСТАВИЛ
Заместитель начальника Управления –
начальник отдела технической защиты
информации и противодействия иностранным
технически разведкам Управления защиты информации и
специальной документальной связи
Аппарата Губернатора Ханты-Мансийского
автономного округа – Югры

_____ Тумаев М.А.

01 ноября 2016г.

1. Общие положения

1. Настоящий документ разработан Управлением специальных мероприятий Аппарата Губернатора Ханты-Мансийского автономного округа – Югры в рамках, возложенных на него полномочий, определенных Положением об Управлении защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры, утвержденного распоряжением Аппарата Губернатора Ханты-Мансийского автономного округа – Югры от 03.02.2016 № 16-р.

2. Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационных систем Аппарата Губернатора Ханты-Мансийского автономного округа – Югры (далее – Аппарат Губернатора Югры) и (или) возникновению угроз безопасности конфиденциальной информации (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима конфиденциальности (далее – служебное расследование) в Аппарате Губернатора Югры.

3. Обеспечение защиты информации в ходе выявления инцидентов и реагирования на них 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 лица, ответственных за обеспечение безопасности информации в Аппарате Губернатора Югры, о возникновении инцидентов в ИС;

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.

4. Процесс управления инцидентами ИБ включает себя:

учет и регистрацию инцидентов ИБ;

оповещение ответственного лица о возникновении инцидентов ИБ;

расследование обнаруженных инцидентов ИБ;

устранение причин и последствий инцидентов ИБ;

определение плана корректирующих и превентивных мероприятий.

5. Требования настоящего Положения являются обязательными для выполнения всеми работниками Аппарата Губернатора Югры.

2. Учет и регистрация инцидентов информационной безопасности

6. Для выявления инцидентов ИБ в Аппарате Губернатора Югры используются встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем Аппарата Губернатора Югры.

7. В обязательном порядке должны регистрироваться следующие события безопасности:

попытки входа (выхода) пользователей в операционную систему (из операционной системы);

загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;

попытка доступа к средствам виртуализации;

факт изменения конфигурации средств виртуализации;

запуск и остановка служб (системных сервисов) средств виртуализации;

попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации;

копирование информации на внешние носители информации.

8. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

тип события;

дата и время события;

результат события;

источник события;

идентификатор пользователя информационной системы, предъявленный при попытке доступа.

9. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

10. Учет инцидентов ИБ осуществляется администратором информационной безопасности Аппарата Губернатора автономного округа (далее – администратор ИБ), назначенным распорядительным документом по Аппарату Губернатора автономного округа. Допускается ведение учета инцидентов ИБ в электронном виде.

11. При обнаружении инцидента ИБ администратор ИБ проводит его классификацию в соответствии с приложением к настоящему Положению.

3. Порядок оповещения о возникновении инцидентов информационной безопасности

12. Средства защиты информации фиксируют инциденты ИБ в системных журналах средств защиты.

При применении средства защиты информации должно обеспечиваться возможность информирования администратора ИБ о критических событиях безопасности в информационной системе по электронной почте или посредством смс информирования.

13. В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», администратор ИБ обязан незамедлительно сообщить о выявленном инциденте ИБ заместителю начальника Управления – начальнику отдела технической защиты информации и противодействия иностранным техническим разведкам (далее – Отдел ТЗИ и ПД ИТР) Управления защиты информации и специальной документальной связи Аппарата Губернатора Югры (далее – Управление ЗИ и СДС).

14. Начальник Отдела ТЗИ и ПД ИТР информирует начальника Управления ЗИ и СДС.

15. Начальник Управления ЗИ и СДС проводит анализ выявленного инцидента ИБ и в случае необходимости докладывает заместителю руководителя Аппарата Губернатора Югры, ответственному за руководство работами по защите информации в Аппарате Губернатора Югры, который в свою очередь инициирует процедуру служебного расследования в соответствии с порядком, установленным в Аппарате Губернатора Югры.

16. В случае обнаружения инцидента ИБ пользователем, руководителем структурного подразделения Аппарата Губернатора Югры, данные лица обязаны незамедлительно поставить в известность администратора ИБ.

4. Порядок расследования обнаруженных инцидентов информационной безопасности

17. Проведение служебного расследования инициируется заместителем руководителя Аппарата Губернатора Югры, ответственного за руководство работами по защите информации в Аппарате Губернатора Югры.

18. Служебное расследование проводится комиссией Аппарата

Губернатора Югры по проведению внутреннего контроля соответствия обработки информации требованиям к обработке и защите информации, установленным федеральным законодательством и принятыми в соответствии с ними нормативными актами, а также локальным актам (далее – Комиссия).

19. Комиссия осуществляет свою деятельность в соответствии с Правилами осуществления в Аппарате Губернатора Ханты-Мансийского автономного округа – Югры внутреннего контроля соответствия обработки информации требованиям к обработке и защите информации, установленным федеральным законодательством и принятыми в соответствии с ними нормативными актами, а также локальным актам, утвержденными заместителем руководителя Аппарата Губернатора Югры, ответственного за руководство работами по защите информации в Аппарате Губернатора Югры.

20. В случае необходимости председатель Комиссии вправе привлекать к расследованию:

администратора информационных систем;

руководителя структурного подразделения, в котором произошел инцидент ИБ;

непосредственного руководителя работника, в отношении которого проводится служебное расследование;

экспертов из других структурных подразделений и, при необходимости, представителей сторонних организаций.

21. Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя руководителя Аппарата Губернатора Югры, с предложениями:

по внесению изменений в организационные и (или) технические меры по защите конфиденциальной информации;

по внесению изменений и улучшений в комплект организационно-распорядительной документации;

по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

22. В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

23. Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами Аппарата Губернатора Югры.

5. Устранение причин и последствий инцидентов информационной безопасности

24. Для инициирования работ по устранению причин и последствий инцидентов ИБ начальник Управления ЗИ и СДС направляет на утверждение руководителю Аппарата Губернатора Югры, согласованные заместителем руководителя Аппарата Губернатора Югры, ответственного за руководство работами по защите информации в Аппарате Губернатора Югры аналитическое экспертное заключение и план мероприятий по устранению выявленных инцидентов ИБ.

Утвержденный план мероприятий по устранению выявленных инцидентов ИБ направляется на исполнение ответственным за выполнение запланированных работ.

25. Если ответственный за выполнение запланированных работ не согласен с установленными сроками, он вправе обратиться к начальнику Управления ЗИ и СДС с просьбой перенести срок с обоснованием причин переноса.

26. При изменении сроков реализации действий, начальник Отдела ТЗИ и ПД ИТР вносит необходимые изменения в экспертное заключение и информирует о них ответственного за выполнение запланированных работ начальника Управления ЗИ и СДС, руководителя структурного подразделения Аппарата Губернатора Югры, заместителя руководителя Аппарата Губернатора Югры, ответственного за руководство работами по защите информации в Аппарате Губернатора Югры и руководителя Аппарата Губернатора Югры.

27 После реализации запланированных работ ответственное лицо должно проинформировать начальника Отдела ТЗИ и ПД ИТР о выполнении работ, не позднее срока реализации, установленного в экспертном заключении.

28. Начальник Отдела ТЗИ и ПД ИТР вправе запросить у исполнителя информацию о выполнении мероприятий по устранению инцидента ИБ в случае, если ему не поступило подтверждение выполнения работ в течение 2 (двух) рабочих дней с даты, установленной в экспертном заключении.

29. Оценку результативности предпринятых мер осуществляет начальник Управления ЗИ и СДС ежеквартально на основании анализа информации, содержащейся в отчетах об инцидентах ИБ, предоставляемого начальников Отдела ТЗИ и ПД ИТР.

30. О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

6. Определение плана корректирующих и превентивных мероприятий

31. Ежемесячно администратор ИБ готовит сводный отчет по инцидентам ИБ, предоставляемый начальнику Отдела ТЗИ и ПД ИТР.

32. В сводном отчете администратор ИБ должен провести анализ выявленных инцидентов ИБ, в качестве приложения к отчету должен быть предложен перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий инцидентов ИБ и на предотвращение подобных нарушений в будущем.

Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.

33. После согласования указанного перечня с начальником Отдела ТЗИ и ПД ИТР, начальником Управления ЗИ и СДС, и утверждения указанного перечня заместителем руководителя Аппарата Губернатора Югры, ответственного за руководство работами по защите информации в Аппарате Губернатора Югры данная информация доводится администратором ИБ до всех работников, назначенных ответственными за проведение корректирующих и превентивных мероприятий.

34. Контроль за своевременным и качественным выполнением работ по проведению корректирующих и превентивных мероприятий осуществляет начальник Отдела ТЗИ и ПД ИТР.

7. Ответственность

35. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор ИБ.

36. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет начальник Отдела ТЗИ и ПД ИТР.

37. Ответственность за выделение требуемых ресурсов (в том числе финансовых и трудовых) для реализации положений настоящего документа несет начальник Управления ЗИ и СДС.

38. Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами Аппарата Губернатора Югры, является грубым нарушением трудовой дисциплины.

39. Работник, осуществляющий автоматизированную обработку информации ограниченного доступа, обязан согласовывать следующие действия с администратором ИБ:

установка дополнительного ПО;

изменение сетевых настроек рабочего места;

замена, изменение любой аппаратной части рабочего места.

40. Никакое должностное лицо Аппарата Губернатора Югры не вправе требовать от администратора ИБ действий, направленных на нарушение настоящего Положения и других документов в области обеспечения безопасности информации, требовать сокрытия инцидентов ИБ, вызванных любыми работников Аппарата Губернатора Югры, требовать сообщения ему паролей и нарушения установленных разрешительной системой разграничения прав по допуску к информационным ресурсам и информации.

Приложение
к Положению о порядке выявления и реагирования
на инциденты информационной безопасности

ПЕРЕЧЕНЬ
инцидентов информационной безопасности
в Аппарате Губернатора Ханты-Мансийского автономного округа - Югры

№ п/п	Описание инцидента информационной безопасности
1	2
1. Текущие нарушения	
1.1.	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная)

1.2.	Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам
1.3.	Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры
1.4.	Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время
1.5.	Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
1.6.	Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания
1.7.	Нецелевое использование элементов информационной инфраструктуры (печать, сервисы сети Интернет, электронная почта, и т.п.)
2. Значимые нарушения	
2.1.	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная)
2.2.	Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
2.3.	Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации
2.4.	Утрата носителя информации с резервной копией
2.5.	Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная)
2.6.	Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)
2.7.	Нерегламентированная очистка журналов событий безопасности информационных систем
2.8.	Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации
2.9.	Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования
2.10.	Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет
2.11.	Нерегламентированная установка (удаление) прикладного

	программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах
2.12.	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем (повышение уровня прав доступа, получение прав на отладку программ и т.п.)
2.13.	Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное)
2.14.	Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения
2.15.	Нерегламентированное использование анализаторов протоколов (снифферов)
2.16.	Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите)
2.17.	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
3. Нарушения, имеющие признаки преступления	
3.1.	Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры
3.2.	Несанкционированное изменение конфигурации элементов информационной инфраструктуры
3.3.	Утрата резервных копий
3.4.	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5.	Подозрение в умышленном нарушении работоспособности информационной сети, элементов информационной инфраструктуры, системного и прикладного программного обеспечения
3.6.	Юридически необоснованная передача (распространение) конфиденциальной информации
3.7.	Несанкционированное внесение изменений в базы данных информационных систем
3.8.	Несанкционированное уничтожение конфиденциальной информации
3.9.	Проведение обновления версии информационных систем (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10.	Намеренное заражение информационных систем вредоносным кодом