Одобрено на заседании

Совета по вопросам технической защиты информации

в Ханты-Мансийском автономном округе – Югре

Протокол от 29.05.2017 № 3/17

Типовые функции и задачи администратора безопасности информации в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры

**1. Общие положения**

1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности (далее – администратор ИБ) информационных систем обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные (далее – ИС) исполнительного органа государственной власти Ханты-Мансийского автономного округа – Югры (далее – орган власти).

2. Администратор ИБ осуществляет контроль выполнения требований организационных и технических мероприятий по обеспечению безопасности информации в ИС.

3. Методическое руководство и контроль работы администратора информационной безопасности органа власти осуществляется отделом технической защиты информации и противодействия иностранным техническим разведкам (далее - Отдел ТЗИ и ПД ИТР) Управления защиты информации и специальной документальной связи (далее – Управление ЗИ и СДС) Аппарата Губернатора Ханты-Мансийского автономного округа – Югры (далее – Аппарат Губернатора Югры).

4. Администратор безопасности назначается приказом по органу власти из числа штатных работников органа власти**.**

5. Администратор ИБ должен принимать все необходимые меры по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных (далее – конфиденциальная информация (КИ)) и контролю за соблюдением прав доступа к ней.

6. Основными задачами при обработке информации в ИС являются:

обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту информации в Российской Федерации в процессе создания, хранения и передачи документов, содержащих конфиденциальную информацию в ИС органа власти;

обеспечение в ИС необходимого уровня безопасности обработки, хранения и передачи КИ;

обеспечение необходимого уровня безопасности носителей КИ;

обеспечение безопасности конфиденциальной информации при ее копировании, размножении;

резервное копирование, восстановление информации.

**2. Обязанности администратора информационной безопасности**

7. Администратор информационной безопасности должен:

знать нормативно-методические документы в области безопасности информации и организационно-распорядительные документы в части его касающейся;

- знать состав ОТСС ИС и контролировать их соответствие техническому паспорту на ИС. Вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения);

- контролировать процесс управления (заведения, активации, блокирования, уничтожения) учетными записями пользователей ИС;

проверять соответствие прав доступа пользователей к объектам доступа ИС в соответствии с задачами, решаемыми пользователями в ИС и взаимодействующими с ней ИС и Разрешительной системой доступа к ИС:

контролировать назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;

проверять отсутствие в ИС учетных записей уволенных (отстраненных) сотрудников;

оповещать администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

проверять своевременность удаления временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС;

- контролировать неизменность настроек средств защиты информации, настройки средств защиты информации должны неизменно выполнять:

препятствие передаче защищаемой информации через сеть Интернет (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи;

ограничение доступа к ИС на 10 минут при 3 неудачных попытках входа в ИС;

запрет доступа к ИС до прохождения процедур аутентификации и идентификации;

обеспечение запрета удаленного доступа к ИС;

- контролировать запрет использования в ИС технологий беспроводного доступа и мобильных технических средств;

- контролировать отсутствие доступа к ИС со стороны пользователей информационных систем сторонних организаций;

- контролировать установку на АРМ ИС ПО не связанного с задачами, решаемыми пользователями в ИС;

- вести учет съемных машинных носителей конфиденциальной информации (далее – СМНКИ);

- обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ ИС, при их передаче в сторонние организации для ремонта или утилизации, либо контролировать процесс уничтожения (стирания), уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

- контролировать регистрацию в ИС следующих событий безопасности:

входа (выхода), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы (дата (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа);

подключения машинных носителей информации и вывода информации на носители информации (дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации);

запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации (дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный));

попыток доступа программных средств к защищаемым объектам доступа (дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип));

попыток удаленного доступа (дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе).

- контролировать права на доступ к информации о событиях безопасности: доступ должен предоставляться исключительно администратору информационной безопасности, а также системному администратору ИС, обеспечивающим функционирование ИС.

- обеспечивать постоянный контроль за выполнением пользователями ИС установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, а также инструкции пользователя и других организационно-распорядительных документов в части обеспечения безопасности информации;

- требовать от пользователей ИС и выполнять самому требования «Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств ИС»;

- контролировать порядок учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

- контролировать использование пользователями только учтенных съемных носителей. После того как цель переноса информации достигнута (переданы третьим лицам и т.п.), информация незамедлительно удаляется с носителей;

- контролировать настройки ОС и СЗИ АРМ пользователей

- проводить инструктаж пользователей по правилам работы с используемыми средствами и системами зашиты информации;

- устанавливать права доступа пользователей к информационным и техническим ресурсам ИС в соответствии с принятой и утвержденной разрешительной системой доступа;

- следить за изменением программной среды ИС и полномочиями пользователей;

- хранить дистрибутивы СЗИ, производить при необходимости восстановление программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИС. При необходимости для данных мероприятий привлекать других технических специалистов отдела ЗИ;

- фиксировать и пресекать невыполнение пользователями ИС требований или норм нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в информационной сфере, а также создания пользователями возможностей утечки информации;

- при получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в том числе с использованием методов социальной инженерии – немедленно докладывать ответственному за организацию обработки персональных данных, инициировать проведение служебной проверки (при нарушениях со стороны ответственного за организацию обработки персональных данных докладывать необходимо непосредственно вышестоящему руководству), регистрировать в журнале учёта инцидентов ИБ.

- не реже 1 раза в квартал просматривать журналы учёта и регистрации событий СЗИ (в соответствии с инструкцией по использованию программных и аппаратных средств защиты информации, операционной системы на предмет выявления подключения неучтённых носителей, попыток НСД и т.п.

- требовать от пользователей ИС и выполнять самому требования инструкции о пропускном и внутриобъектовом режимах в здании органа власти.

- контролировать отсутствие в составе ПО АРМ, входящих в ИС, средств разработки и отладки программ.

- реагировать на поступление в ИС спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

- выполнять мероприятия по периодическому резервному копированию защищаемой информации в соответствии с «Инструкцией по резервному копированию и восстановлению данных».

- знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией.

- хранить документацию и дистрибутивы СЗИ в соответствии с техническими условиями. Компакт-диск с программным обеспечением системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей;

- поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом система должна реализовывать в совокупности на каждой АРМ ИС функции необходимые для выполнения требований по защите от НСД для ИС;

- контролировать срок действия сертификатов соответствия на СЗИ и обеспечить их продление в соответствии с порядком продления, приведённым ниже.

8. Администратор ИБ оказывает методическую помощь и контролирует выполнение руководителем структурного подразделения, эксплуатирующего ИС следующих действий:

при смене пользователя руководитель структурного подразделения, эксплуатирующего ИС, инициирует внесение изменений в список работников, допущенных к работе в данной ИС и в разрешительную систему доступа;

при исключении пользователя ИС из «Перечня лиц, имеющих доступ к самостоятельной работе в ИС» руководителем подразделения, эксплуатирующего ИС, принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности информации ИС.

Администратору информационной безопасности необходимо до момента доведения до сотрудника информации о прекращении его работы в ИС, лишить сотрудника возможности доступа к защищаемой информации.

9. Администратору ИБ **запрещается**:

фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя;

раскрывать информацию об организации СЗ КИ в органе власти и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

**3. Права администратора информационной безопасности**

10. Требовать от пользователей ИС соблюдения установленных технологий обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов на ИС;

11. Давать своему непосредственному начальнику предложения по совершенствованию мер защиты в ИС;

12. Инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации;

**4. Ответственность**

13. Администратор ИБ несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности.

14. Ответственность за защиту ИС от несанкционированного доступа к информации и за неукоснительное соблюдение положений настоящего руководства возлагается на администратора информационной безопасности.

**5. Инструкция администратора информационной безопасности по работе с инцидентами информационной безопасности**

15. Для регистрации и учета событий, которые могут привести к снижению уровня защищенности информации (далее – инцидент), в органе власти используются встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также применяться средства (системы) анализа защищенности.

16. В органе власти обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС.

Средства (системы) анализа защищенности должны обеспечивать, в том числе:

выявление и анализ уязвимостей, связанных с ошибками в конфигурации операционных систем и программного обеспечения рабочих станций и серверов ИС органа власти;

контроль установки обновлений программного обеспечения рабочих станций и серверов ИС органа власти.

17. Анализ инцидентов осуществляется:

администратором безопасности при просмотре журналов событий, формируемых средствами защиты информации, журналов событий, формируемых программным обеспечением ИС и системами управления базами данных;

системными администраторами при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

18. Журналы аудита СЗИ от НСД и СКЗИ просматриваться администратором безопасности не реже одного раза в две недели.

19. О фактах обнаружения инцидентов администратор безопасности органа власти докладывает непосредственному руководителю, начальнику Отдела ТЗИ и ПД ИТР.

20. Управление инцидентами информационной безопасности и реагирование на них в органе власти осуществляется в соответствии с Положением о порядке выявления и реагирования на инциденты информационной безопасности в органе власти.