

Утверждено

Приказом министерства жилищно-коммунального хозяйства и топливно-энергетического комплекса Новгородской области

от «__» _____ 2019 г. № _____

ПОЛОЖЕНИЕ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ МИНИСТЕРСТВА
ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

СОДЕРЖАНИЕ

| | |
|--|----|
| ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ | 5 |
| ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ | 12 |
| 1. ОБЛАСТЬ ДЕЙСТВИЯ | 13 |
| 2. ОБЩИЕ ПОЛОЖЕНИЯ | 13 |
| 2.1. Цели и задачи обеспечения безопасности персональных данных | 13 |
| 2.2. Порядок пересмотра Положения..... | 14 |
| 2.3. Декларация о поддержке Положения | 15 |
| 3. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ | 16 |
| 3.1. Принятие решений..... | 16 |
| 3.2. Анализ функционирования системы защиты информации | 17 |
| 3.3. Порядок определения ролей персонала ИСПДн МЖКХиТЭК | 17 |
| 4. ОБЯЗАННОСТИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ | 20 |
| 4.1. Распределение обязанностей | 20 |
| 4.2. Ответственный за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК..... | 20 |
| 4.3. Руководители подразделений | 22 |
| 4.4. Администратор безопасности ИСПДн МЖКХиТЭК | 22 |
| 4.5. Обязанности системного администратора | 25 |
| 4.6. Обязанности сотрудников..... | 26 |
| 4.7. Обязанности сотрудников, наделенных правами приеме на работу и увольнения | 27 |
| 5. УПРАВЛЕНИЕ ДОСТУПОМ | 28 |
| 5.1. Управление и контроль доступа..... | 28 |
| 5.2. Управление паролями..... | 29 |
| 5.3. Правила формирования пароля | 31 |
| 5.4. Действия в случае компрометации пароля..... | 31 |
| 5.5. Политика «чистого» стола и очистки экрана | 32 |
| 5.6. Правила предоставления доступа к ресурсам ИСПДн МЖКХиТЭК | 32 |
| 5.7. Правила локального доступа к ресурсам..... | 34 |
| 5.8. Правила удаленного доступа к ресурсам ИСПДн МЖКХиТЭК..... | 35 |
| 5.9. Правила формирования матрицы доступа к ресурсам ИСПДн МЖКХиТЭК | 36 |
| 5.10. Контроль обработки конфиденциальной информации | 40 |
| 6. АНТИВИРУСНАЯ ЗАЩИТА | 41 |

| | | |
|---------|---|----|
| 6.1. | Общие требования к антивирусной защите | 41 |
| 6.2. | Правила применения средств антивирусной защиты..... | 41 |
| 6.3. | Требования к процессам функционирования подсистемы антивирусной защиты | 42 |
| 7. | ИСПОЛЬЗОВАНИЕ НЕКОНТРОЛИРУЕМЫХ РЕСУРСОВ СЕТИ ИНТЕРНЕТ | 43 |
| 7.1. | Общие требования к организации доступа к сети Интернет..... | 43 |
| 7.2. | Порядок получения доступа в режиме on-line | 44 |
| 7.3. | Порядок получения доступа в режиме off-line..... | 44 |
| 8. | УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ СЕТЕВЫХ РЕСУРСОВ | 46 |
| 8.1. | Общие требования по обеспечению безопасности сетевых ресурсов | 46 |
| 8.2. | Организация сетевой защиты ЛВС ИСПДн МЖКХиТЭК..... | 47 |
| 8.3. | Защита каналов связи | 48 |
| 8.4. | Безопасность сетевых служб..... | 51 |
| 9. | КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ | 53 |
| 9.1. | Контроль текущего состояния защищенности ИСПДн МЖКХиТЭК..... | 53 |
| 9.2. | Комплексное обследование состояния защищенности ИСПДн МЖКХиТЭК | 54 |
| 9.3. | Обнаружение вторжений в процессы функционирования ИСПДн МЖКХиТЭК.. | 56 |
| 10. | ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ | 58 |
| 10.1. | Общие требования к использованию мобильных технических средств | 58 |
| 10.2. | Организация учета съемных носителей информации | 58 |
| 10.3. | Организация хранения и выдачи съемных носителей информации..... | 59 |
| 10.4. | Организация уничтожения съемных носителей информации..... | 59 |
| 11. | ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ | 61 |
| 12. | БЕЗОПАСНОСТЬ ИНФОРМАЦИИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА | 62 |
| 12.1. | Требования по обеспечению безопасности информации в ИСПДн МЖКХиТЭК на стадиях жизненного цикла..... | 62 |
| 12.2. | Взаимодействие с внешними организациями | 64 |
| 12.2.1. | Идентификация рисков, связанных с привлечением внешней стороной | 64 |
| 12.2.2. | Защита информационных ресурсов при работе с внешней стороной | 66 |
| 12.2.3. | Соглашения о конфиденциальности | 67 |
| 12.3. | Планирование и приемка компонентов подсистем защиты информации..... | 69 |
| 12.3.1. | Принятие систем (компонентов системы) защиты информации | 70 |
| 12.3.2. | Процесс подключения новых средств защиты информации | 71 |
| 12.4. | Безопасность разработки и сопровождения программного обеспечения | 71 |
| 12.4.1. | Управление изменениями конфигураций средств защиты информации | 72 |

| | | |
|--------------|--|----|
| 12.4.2. | Технологическая проверка прикладного программного обеспечения после изменений (обновлений) операционной системы | 73 |
| 12.4.3. | Ограничения на изменения пакетов используемого программного обеспечения | 74 |
| 12.4.4. | Вопросы утечки информации в ходе разработки и сопровождения программного обеспечения | 75 |
| 12.4.5. | Вопросы защиты информации при разработке программного обеспечения внешней стороной | 75 |
| 13. | ТРЕБОВАНИЯ К ОРГАНИЗАЦИЯМ, ПРЕДОСТАВЛЯЮЩИМ УСЛУГИ ПО СОПРОВОЖДЕНИЮ, ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ, МОДЕРНИЗАЦИИ И ВНЕДРЕНИЮ НОВЫХ СИСТЕМ И СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ, ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ | 77 |
| 13.1. | Требования к размещению СВТ с которых разрешен удаленного доступа из информационных систем подрядных организаций..... | 78 |
| 13.2. | Требования к хранению бумажных и машинных носителей с конфиденциальной информацией, переданной Министерством подрядной организации | 78 |
| 13.3. | Требования к программно-аппаратной среде СВТ с которых разрешен удаленного доступа из информационных систем подрядных организаций..... | 78 |
| 13.4. | Требования к средствам защиты АРМ подрядной организации, с которых разрешен удаленного доступа к СВТ ИСПДн МЖКХиТЭК..... | 79 |
| 14. | УПРАВЛЕНИЕ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ | 80 |
| 15. | ОБУЧЕНИЕ И ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ ПЕРСОНАЛА ИСПДн МЖКХиТЭК..... | 82 |
| 15.1. | Общие положения..... | 82 |
| 15.2. | Вводный инструктаж | 82 |
| 15.3. | Первичный инструктаж | 83 |
| 15.4. | Внеплановый инструктаж | 83 |
| 15.5. | Формы проведения занятий | 84 |
| Приложение 1 | Форма заявки..... | 85 |
| Приложение 2 | Формы журналов..... | 86 |
| Приложение 3 | Правила закупки..... | 88 |
| Приложение 4 | Типовые действия при инцидентах безопасности информации | 91 |
| Приложение 5 | Пример договора о соблюдении конфиденциальности переданных персональных данных | 98 |

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

| | |
|---|--|
| Автоматизированная система (АС) | система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций |
| Атака на систему [attack, intrusion] | действие или последовательность связанных между собой действий источника угроз с использованием уязвимостей, которые приводят к реализации целей атаки |
| Аутентификация | проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности) |
| Информационный технологический процесс | часть технологического процесса, реализующая операции по изменению и (или) определению состояния информационных ресурсов, необходимых для функционирования информационной системы |
| Технологический процесс | процесс, реализующий операции по изменению и (или) определению состояния ресурсов информационной системы |
| Безопасность информации | состояние защищенности интересов (целей) организации в условиях угроз безопасности информации |
| Блокирование компьютерной информации (блокирование) | искусственное затруднение доступа пользователей к защищаемой информации, не связанное с ее уничтожением |
| Допустимый риск | риск, который в данной ситуации считается приемлемым для руководства |
| Допустимый риск нарушения информационной безопасности | риск нарушения информационной безопасности, предполагаемый ущерб который организация в данное время и в данной ситуации готова принять |
| Доступность информационных ресурсов | свойство информации, состоящее в том, что информационные ресурсы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы |
| Доступ к информации (Доступ) | ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации |
| Защищаемая информация | информация, подлежащая защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми владельцем информационной системы |
| Защищаемые помещения | помещения (служебные кабинеты, актовые, конференц-залы), |

| | |
|--|--|
| Защитная мера | специально предназначенные для проведения закрытых мероприятий (совещаний, обсуждений, конференций, переговоров), а также помещения, оборудованные средствами правительственной связи, иных видов специальной связи сложившаяся практика, процедура или механизм, которые используются для уменьшения риска проявления угроз безопасности информации |
| Информация | сведения (сообщения, данные) независимо от формы их представления ¹ |
| Информационная безопасность | безопасность, связанная с угрозами в информационной сфере |
| Информационная инфраструктура (инфраструктура) | система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия Информационная инфраструктура: - включает совокупность информационных центров, банков данных и знаний, систем связи; - обеспечивает доступ потребителей к информационным ресурсам. |
| Информационная система | организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе использующих средства вычислительной техники и связи |
| Информационная система персональных данных (ИСПДн) | информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств ² |
| Информационная услуга | действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами |
| Информационные ресурсы | отдельные документы, отдельные массивы документов, документы или массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) |
| Информационная технология (ИТ) | совокупность методов, способов, приемов и средств обработки документированной информации и регламентированного |

¹ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

² Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», ст.2

| | |
|--|--|
| | порядка ее применения |
| Инцидент безопасности | событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы |
| Контролируемая зона | пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств |
| Конфиденциальность информационных ресурсов | свойство безопасности, состоящее в том, что обработка, хранение и передача информационных ресурсов осуществляются таким образом, что информационные ресурсы доступны только авторизованным пользователям, объектам системы или процессам |
| Мониторинг информационной безопасности | оперативное и постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения в соответствии с заданными целями |
| Модель угроз информационной безопасности (модель угроз) | описание источников угроз информационной безопасности; методов реализации угроз информационной безопасности; объектов, пригодных для реализации угроз информационной безопасности; уязвимостей, используемых источниками угроз информационной безопасности; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба |
| Модификация компьютерной информации (модификация) | внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных |
| Мониторинг | постоянное наблюдение за объектами и субъектами, влияющими на безопасность информационной системы, а также сбор, анализ и обобщение результатов наблюдений |
| Нарушитель информационной безопасности | субъект, реализующий угрозы безопасности информации, нарушая предоставленные ему полномочия по доступу к ресурсам информационной системы или по распоряжению ими |
| Несанкционированный доступ к информации | доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств ³ , предоставляемых средствами вычислительной техники или автоматизированными системами |

³ Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

Министерство жилищно-коммунального хозяйства и топливно-энергетического комплекса
Новгородской области

| | |
|--|--|
| Обладатель информации | лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам ⁴ |
| Обработка персональных данных | действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных ⁵ |
| Объект защиты информации | информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации |
| Оператор информационной системы | гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных |
| Оператор персональных данных | государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных ⁶ |
| Оценка риска нарушения безопасности информации | систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения безопасности информации, связанных с использованием информационных ресурсов на всех стадиях их жизненного цикла |
| Персональные данные | любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация ⁷ |
| Подсистема защиты информации | взаимоувязанный комплекс организационных мер, программных и программно-технических средств, обеспечивающих защиту от |

⁴ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ст.2

⁵ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», ст.2

⁶ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», ст.2

⁷ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», ст.2

| | |
|---|---|
| | случайных и преднамеренных угроз, в результате реализации которых возможно нарушение доступности, целостности или конфиденциальности обрабатываемой информации. |
| Политика информационной безопасности | Совокупность устных, письменных и иных форм представления требований по обеспечению безопасности информации |
| Пользователь информации (потребитель) | субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею |
| Программное обеспечение | объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата |
| Процесс | совокупность взаимосвязанных ресурсов и деятельности, преобразующая входы в выходы |
| Регистрация | фиксация данных о совершенных действиях (событиях) |
| Роль | заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом |
| Информационный риск (риск нарушения безопасности информации) | риск, связанный с проявлениями угроз безопасности информации |
| Ресурс | актив организации, который используется или потребляется в процессе выполнения некоторой деятельности |
| Санкционированный доступ ⁸ | доступ к информации, не нарушающий правила разграничения доступа |
| Свидетельства выполнения деятельности по обеспечению безопасности | документ или часть документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению безопасности информации |
| Система | множество (совокупность) материальных объектов (элементов) любой, в том числе различной физической, природы и информационных объектов, взаимодействующих между собой для достижения общей цели, обладающее системным свойством (свойствами) |
| Система защиты информации | совокупность организационных и технических мер и средств обеспечения безопасности информации |
| Субъект доступа | лицо или процесс, действия которого регламентируются |

⁸ Руководящий документ. Гостехкомиссия России Защита от несанкционированного доступа к информации. Термины и определения

| | |
|---|--|
| | правилами разграничения доступа |
| Субъект информационных отношений | граждане, юридические лица, органы государственной власти и местного самоуправления, участвующие в создании, сборе, обработке, накоплении, хранении, поиске, распространении и предоставлении информации |
| Средство защиты информации | технические, криптографические, программные и другие средства, предназначенные для защиты информационных ресурсов, а также средства контроля эффективности защиты информации |
| Угроза информационной безопасности | угроза нарушения свойств информационной безопасности - доступности, целостности или конфиденциальности информации |
| Уничтожение | внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота. Относительно информации – любое не разрешенные законом, собственником или компетентным пользователем уничтожение защищаемой информации, в том числе стирание в памяти основным технических средств и систем (технических средств) или уничтожение документов |
| Управление информационной безопасностью | совокупность целенаправленных действий, осуществляемых с целью снижения риска в информационной сфере до приемлемого уровня |

Примечания

1. Совокупность действий включает оценку ситуации и состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и реализацию (планирование, внедрение и обслуживание защитных мер (средств управления информационной безопасностью)).
2. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений.

Министерство жилищно-коммунального хозяйства и топливно-энергетического комплекса
Новгородской области

| | |
|--|---|
| Ущерб | утрата ресурсов информационной системы, повреждение (утрата свойств) ресурсов и (или) инфраструктуры информационной системы или другой вред ресурсам и (или) инфраструктуре информационной системы, наступивший в результате реализации угроз безопасности информации через имеющиеся место уязвимости |
| Хищение | совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества. Относительно информации – кража, в том числе с использованием специальных технических и программных средств или завладение мошенническим способом информацией или документами. |
| Цель обеспечения безопасности информации | предмет стремления, то, что надо осуществить при организации обеспечения безопасности информации |
| Целостность информационных ресурсов | свойство сохранять неизменность или исправлять обнаруженные изменения |

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

| | |
|--------------|---|
| АС | автоматизированная информационная система |
| ИТ | информационные технологии |
| ЛВС | локальная вычислительная сеть |
| Министерство | Министерство жилищно-коммунального хозяйства и топливно-энергетического комплекса |
| ПО | программное обеспечение |
| СВТ | средства вычислительной техники |
| СУБД | система управления базами данных |
| ФСБ России | Федеральная служба безопасности России |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |

1. ОБЛАСТЬ ДЕЙСТВИЯ

Настоящее Положение по обеспечению информационной безопасности в информационной системе персональных данных Министерства жилищно-коммунального хозяйства и топливно-энергетического комплекса Новгородской области (далее Положение) является организационно-распорядительным документом Министерства жилищно-коммунального хозяйства и топливно-энергетического комплекса Новгородской области (далее Министерство), в котором изложены цели, требования, правила и положения, определяющие порядок организации и обеспечения защиты персональных данных и иной защищаемой информации⁹ в информационной системе персональных данных Министерства (далее – ИСПДн МЖКХиТЭК).

Настоящее Положение разработано в соответствии с требованиями федерального законодательства Российской Федерации, нормативно-правовых актов органов государственной власти Российской Федерации и внутренних организационно-распорядительных документов Министерства и предназначено для использования в ИСПДн МЖКХиТЭК, а также в подрядных организациях, принимающих участие в проектировании, создании, эксплуатации систем безопасности ИСПДн МЖКХиТЭК.

ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Цели и задачи обеспечения безопасности персональных данных

Целями обеспечения безопасности персональных данных в ИСПДн МЖКХиТЭК является исключение возможности нанесения материального, морального и иного случайного или преднамеренного ущерба (вреда) субъектам персональных данных и иным участникам информационного процесса, в результате нарушения конфиденциальности, целостности и доступности обрабатываемых в ИСПДн МЖКХиТЭК персональных данных и иной защищаемой информации, обеспечение безопасности которой является необходимым условием целостности процессов функционирования ИСПДн МЖКХиТЭК.

Выполнение требований настоящего Положения обеспечивает минимизацию рисков проявления угроз информационной безопасности обрабатываемых в ИСПДн МЖКХиТЭК персональных данных.

⁹ Под защищаемой информацией здесь и далее по тексту документа понимается информация, обрабатываемая, хранимая и передаваемая по каналам связи, нарушение конфиденциальности, целостности и доступности которой приводит к реализации (проявлению) угроз информационной безопасности

Выполнение требований и правил Положения при создании, модернизации и эксплуатации автоматизированных систем и комплексов связи, составляющих инфраструктуру ИСПДн МЖКХиТЭК, должно быть направлено на обеспечение эффективного решения следующих задач:

- Защита от вмешательства в процессы функционирования ИСПДн МЖКХиТЭК посторонних лиц.
- Защита от несанкционированных действий с информационными ресурсами ИСПДн МЖКХиТЭК посторонних лиц и работников, не имеющих полномочий.
- Обеспечение полноты, достоверности и оперативности информационной поддержки принятия решений руководством Министерства по вопросам обеспечения информационной безопасности.
- Регистрация событий, влияющих на безопасность Персональных данных информации и другой защищаемой информации, обеспечение подконтрольности и подотчетности выполнения критичных операций, выполняемых с использованием средств обработки информации.
- Выявление и прогнозирование угроз информационной безопасности, причин и условий, способных нанести вред субъектам персональных данных и иным участникам информационных процессов.
- Предотвращение неприемлемых последствий как результат нарушения требований обеспечения безопасности персональных данных, создание условий для минимизации и локализации наносимого ущерба.
- Обеспечение возможности восстановления актуального состояния инфраструктуры ИСПДн МЖКХиТЭК в случае нарушений установленного режима обеспечения информационной безопасности.

ИСПДн МЖКХиТЭК должна соответствовать требованиям, предъявляемым к информационным системам персональных данных, не ниже 3 уровня защищенности обрабатываемых персональных данных.

2.2. Порядок пересмотра Положения

Пересмотр (актуализация) Положения проводится ежегодно в запланированные интервалы времени на основе результатов независимых анализов и экспертиз; информации об изменении статуса превентивных и корректирующих действий; результатов расследования инцидентов и происшествий, рекомендации, полученные от

органов государственной власти Российской Федерации и должен учитывать необходимость совершенствования и дальнейшее развитие системы защиты персональных данных в ИСПДн МЖКХиТЭК.

Все изменения Положения вносятся приказами Министерства жилищно-коммунального хозяйства и топливно-энергетического комплекса Новгородской области.

2.3. Декларация о поддержке Положения

Руководство Министерства понимает и принимает на себя ответственность за реализацию и поддержку в актуальном состоянии процессов обеспечения безопасности персональных данных и иной защищаемой информации, обрабатываемой в ИСПДн МЖКХиТЭК.

Руководство Министерства являясь оператором персональных данных несет всю полноту ответственности за выполнение требований законодательства Российской Федерации и полномочных органов государственной власти за обеспечение безопасности персональных данных граждан и иных физических лиц субъектов персональных данных.

В связи этим Министерства берет на себя ответственность за выполнение требований законодательства Российской Федерации в области защиты информации, в том числе персональных данных, обрабатываемых в ИСПДн МЖКХиТЭК.

Для выполнения требований по реализации и поддержки в актуальном состоянии процессов обеспечения безопасности персональных данных в ИСПДн МЖКХиТЭК Министерство устанавливает режим защиты информации и обеспечивается контроль его выполнения всеми участниками информационных процессов в ИСПДн МЖКХиТЭК.

2. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИИ

Управление процессами обеспечения информационной безопасности в ИСПДн МЖКХиТЭК является частью системы управления деятельностью сотрудников Министерства и основывается на осознании персоналом ИСПДн МЖКХиТЭК необходимости выполнения требований по защите обрабатываемых в ней персональных данных.

Управление процессами обеспечения безопасности персональных данных осуществляется в условиях:

- штатного функционирования ИСПДн МЖКХиТЭК;
- возникновения аварий, локальных инцидентов и проблем обеспечения безопасности информации;
- ввода новых и модернизации, используемых в ИСПДн МЖКХиТЭК, систем и средств обработки информации.

Организация процессов управления безопасностью информации в ИСПДн МЖКХиТЭК реализуется в виде совокупности взаимозависимых и постоянно действующих процедур (контроля, мониторинга, анализа) штатного функционирования используемых защитных мер и должного исполнения персоналом ИСПДн МЖКХиТЭК предъявляемых к ним требований к обеспечению безопасности персональных данных и иной защищаемой информации.

Действия по обеспечению информационной безопасности в ИСПДн МЖКХиТЭК координируются ответственным за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК во всех структурных подразделениях Министерства, принимающих участие в процессах функционирования ИСПДн МЖКХиТЭК.

Координация мер по обеспечению информационной безопасности должна учитывать процессы взаимодействия руководителей разных звеньев, пользователей, администраторов, проектировщиков, ревизоров (контролеров), а также сотрудников с правами администратора безопасности ИСПДн МЖКХиТЭК.

3.1. Принятие решений

Решение о вводе в эксплуатацию систем и средств защиты информации в ИСПДн МЖКХиТЭК, в том числе их компонентов, утверждается приказом Министерства и основывается на документально оформленных протоколах, подтверждающих:

- выполнение организационно-технических мер защиты информации;

- распределение ролей персонала ИСПДн МЖКХиТЭК;
- выделение ресурсов, необходимых для эксплуатации ИСПДн МЖКХиТЭК.

Процедуры назначения и распределения ролей для всех структурных подразделений Министерства и персонала ИСПДн МЖКХиТЭК, а также персонала обеспечивающих систем, имеющего доступ к ресурсам внедряемых систем и средств защиты информации, принимаются на основании решения руководства Министерства.

3.2. Анализ функционирования системы защиты информации

В ИСПДн МЖКХиТЭК регулярно (не реже 1 раза в год) должен проводиться анализ состояния процессов функционирования системы защиты персональных данных. Анализ проводится ответственным за обеспечение информационной безопасности на основе:

- результатов мониторинга состояния защищенности ИСПДн МЖКХиТЭК;
- сведений об инцидентах безопасности.

Анализ включает в себя:

- проверку адекватности используемых защитных мер;
- проверку отсутствия разрывов в технологических процессах обеспечения безопасности информации, а также несогласованности в процедурах использовании защитных мер.

Полученные результаты анализа документируются.

3.3. Порядок определения ролей персонала ИСПДн МЖКХиТЭК

Роль – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом доступа (работником) и объектом (программно-аппаратным средством).

Роли зарегистрированных пользователей и обслуживающего персонала ИСПДн МЖКХиТЭК и их обязанности должны:

- применяться в конкретных информационных технологиях, определяющих использование ресурсов ИСПДн МЖКХиТЭК, в соответствии организационно-распорядительными документами Министерства (положениями, обязанностями, инструкциями и регламентами);
- обеспечивать защиту от несанкционированного доступа, раскрытия, модификации или уничтожения информации;
- определять специальные действия (действия в нештатных ситуациях);

- устанавливать персональную ответственность участников информационного взаимодействия за выполненные действия;
- основываться на требованиях к минимизации информационных рисков.

Роли доводятся до сотрудников Министерства до начала их работы в ИСПДн МЖКХиТЭК.

До пользователей, представляющих внешнюю сторону, а также до лиц, не имеющих правовых отношений с Министерством, но зарегистрированных в ИСПДн МЖКХиТЭК, роли и обязанности доводятся через соответствующие соглашения о соблюдении мер к обеспечению безопасности информации при работе с ресурсами ИСПДн МЖКХиТЭК.

Роли персонифицируются с установлением ответственности за их исполнение. Формирование ролей выполняется в соответствии с требованиями технологических процессов ИСПДн МЖКХиТЭК. Персонифицированная роль субъекта фиксируется в должностных инструкциях сотрудника Министерства.

Запрещается применять ролевой механизм, где одна персональная роль включает права, обеспечивающие полный доступ ко всем операциям по администрированию, сопровождению и/или обслуживанию более одного технологического процесса. Совокупность правил, определяющих ту или иную роль, не должна быть критичной для ИСПДн МЖКХиТЭК с точки зрения последствий успешного ее применения злоумышленником и/или инициированным им процессом.

При определении ролей для работников, работающих по контракту и третьей стороны необходимо учитывать целевые задачи, стоящие перед Министерством, функциональные и процедурные требования, критерии оценки эффективности выполнения правил для данной роли.

Ненадлежащее выполнение правил по назначению и распределению ролей субъектов доступа является проявлением угрозы безопасности информации в ИСПДн МЖКХиТЭК.

Для контроля требований выполнения процедур назначения и распределения ролей персонала ИСПДн МЖКХиТЭК определяются роли контролеров – аудиторов контроля состояния защищенности ИСПДн МЖКХиТЭК.

В случае изменения статуса (должностного положения) сотрудника из числа персонала ИСПДн МЖКХиТЭК, работника по контракту или представителя внешней стороны с правами доступа к ресурсам ИСПДн МЖКХиТЭК, администратор

безопасности ИСПДн МЖКХиТЭК обязан выполнить процедуры перераспределения прав или удаления ранее предоставленной учетной записи пользователя.

Процедура перераспределения прав доступа должна включать в себя удаление (блокирование с последующим удалением) существующей учетной записи и создание новой, либо перераспределение атрибутов и прав доступа для существующей учетной записи пользователя.

Изменения должны отражаться в удалении всех прав доступа, которые не одобрены для новой занятости (должности). Права доступа, которые должны быть удалены или адаптированы, включают физический и логический доступ, ключи, идентификационные средства, средства обработки информации, подписки, и уничтожение любых документов, которые идентифицирует их как документы действующего субъекта доступа к ресурсам ИСПДн МЖКХиТЭК. Если удаление учетной записи субъекта доступа после изменения его занятости не представляется возможным, то используемая им ранее аутентификационная информация (например, пароли доступа) должна быть изменена.

В случае увольнения сотрудника из числа персонала ИСПДн МЖКХиТЭК, служащего по контракту или представителя внешней стороны с правами доступа к ресурсам ИСПДн МЖКХиТЭК, администратор безопасности ИСПДн МЖКХиТЭК обязан гарантировано заблокировать пользовательский вход увольняемого, а через 30 суток удалить его учетную запись.

Права доступа к ресурсам ИСПДн МЖКХиТЭК должны быть прекращены или удалены прежде, чем у увольняемого или переходящего на другую работу субъекта доступа может появиться возможность уничтожить или изменить их самому.

3. ОБЯЗАННОСТИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4.1. Распределение обязанностей

Обязанности пользователей ИСПДн МЖКХиТЭК отражаются в должностных инструкциях сотрудников Министерства, включаются в трудовые соглашения между работником и Министерством и определяют их ответственность, а также порядок и правила работы с предоставленными им ресурсами ИСПДн МЖКХиТЭК и порядок доступа к этим ресурсам в соответствии с назначенной ролью.

Руководители подразделений (отделов Министерства) могут делегировать часть своих полномочий и обязанностей другим должностным лицам с определением порядка их подотчетности и ответственности. Руководители, делегировавшие часть своих полномочий, остаются ответственными и должны контролировать выполнение делегированных ими обязанностей.

Обязанности руководителя подразделения включают указания на информационные и другие ресурсы, а также технологические процессы, ответственность за которые возлагается на соответствующего руководителя.

В обязанности сотрудников Министерства из числа персонала ИСПДн МЖКХиТЭК включаются требования об ответственности за разглашение конфиденциальных сведений, в частности персональных данных, ставших известными входе выполнения сотрудником своих должностных обязанностей, сроки и условия сохранения известных ему защищаемых сведений.

4.2. Ответственный за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК

Общее руководство по обеспечению информационной безопасности в ИСПДн МЖКХиТЭК осуществляет Ответственный за обеспечение информационной безопасности.

Ответственный за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК отвечает за:

- проведение анализа информационных потоков ИСПДн МЖКХиТЭК, с целью выявления имеющих место недостатков в организации принятых мер защиты, составление и организацию исполнения планов по их устранению;

- проведение анализа состояния информационных ресурсов ИСПДн МЖКХиТЭК, определение требований к защищенности различных систем и средств обработки, хранения и передачи информации, а также осуществление выбора методов и средств обеспечения их защиты;
- организацию своевременного прогнозирования, выявления и оценки источников угроз безопасности информации, причин и условий их проявления, способствующих нанесению ущерба интересам субъектов, чьи персональные данные обрабатываются в ИСПДн МЖКХиТЭК;
- организацию разработки внутренних организационно-распорядительных документов, определяющих политику информационной безопасности, регламентирующих порядок, требования и правила обеспечения безопасности информации в ИСПДн МЖКХиТЭК;
- координацию работы всех обслуживающих ИСПДн МЖКХиТЭК подразделений, а также внешних организаций, предоставляющих услуги сопровождения и модернизации ИСПДн МЖКХиТЭК, по вопросам обеспечения безопасности информации, а также координацию деятельности системных администраторов и администратора безопасности;
- организацию взаимодействия с подразделениями безопасности организаций, использующих информационные ресурсы ИСПДн МЖКХиТЭК, а также с подразделениями организаций, предоставляющих свои ресурсы для их использования в ИСПДн МЖКХиТЭК;
- организацию и контроль выполнения работ по совершенствованию документов, определяющих порядок выполнения технологических операций по предоставлению прав доступа к информационным ресурсам ИСПДн МЖКХиТЭК и к средствам обработки информации;
- организацию финансового планирования деятельности по обеспечению безопасности информации, проведения оценки потребности в технических средствах защиты и контроля состояния защищенности, составления заявок на их приобретение с необходимыми обоснованиями и расчетами к ним, контроль их поставки;
- организацию разработки и своевременного представления предложений для включения в соответствующие разделы перспективных и текущих планов работ и программ мер по контролю и защите информации;

- организацию обучения, переподготовки и повышения квалификации сотрудников Министерства из числа персонала ИСПДн МЖКХиТЭК по вопросам обеспечения информационной безопасности.

4.3. Руководители подразделений

Руководители подразделений Министерства, отвечающие за организацию и управление процессами функционирования ИСПДн МЖКХиТЭК, несут полную ответственность за выполнение подчиненными им работниками положений и требований по обеспечению безопасности информации.

Руководители подразделений Министерства обязаны:

- постоянно держать в поле зрения вопросы обеспечения безопасности в ИСПДн МЖКХиТЭК, следить за выполнением подчиненными требований по обеспечению безопасности;
- определять информационные ресурсы, находящиеся в зоне их ответственности, подлежащие защите;
- выявлять недостатки системы защиты информации, оценивать размер потенциального ущерба от возможного нарушения установленного режима защиты информации;
- следить за состоянием, используемых подчиненными физических, инженерно-технических и программно-технических средств и систем защиты;
- организовывать информирование подчиненных по вопросам обеспечения безопасности информации;
- информировать руководство об имеющихся проблемах и фактах неэффективного использования мер и средств защиты.

4.4. Администратор безопасности ИСПДн МЖКХиТЭК

Администратор безопасности ИСПДн МЖКХиТЭК обязан:

- обеспечивать режим безопасности информации при осуществлении всех видов деятельности, связанных с информационными ресурсами, подлежащих защите;
- управлять системой защиты информации ИСПДн МЖКХиТЭК, обеспечивать использование средств и систем защиты информации в соответствии с требованиями проектной и эксплуатационной документации, а также настоящего Положения,

- выполнять работы по установке, настройке, администрированию и сопровождению специализированных средств защиты информации, обеспечивать техническую поддержку средств защиты информации, сопровождаемых системными администраторами, хранения и передачи информации, антивирусных средств защиты, контролировать состояние технологий обеспечения защиты сетевых ресурсов на уровне каналообразующего оборудования, в том числе технологии VLAN;
- проводить мероприятия по выявлению и устранению уязвимостей в ИСПДн МЖКХиТЭК, по сбору статистических данных для анализа и выявления источников угроз; проводить сканирование сетевых ресурсов с целью выявления уязвимостей в используемых технологиях;
- организовывать и управлять предоставлением прав доступа к ресурсам ИСПДн МЖКХиТЭК, организовывать учет, хранение и выдачу съемных носителей информации, контролировать выполнение требований парольной защиты, правил работы с ключами, используемых в ИСПДн МЖКХиТЭК;
- осуществлять обеспечение безопасной эксплуатации средств криптографической защиты информации;
- обеспечивать возможности восстановления актуального состояния информационных ресурсов ИСПДн МЖКХиТЭК при нарушении безопасности информации и ликвидации последствий этих нарушений, выполнять работы по сопровождению библиотеки дистрибутивов критичного для функционирования ИСПДн МЖКХиТЭК программного обеспечения;
- осуществлять периодический контроль соблюдения системным администратором ИСПДн МЖКХиТЭК требований к процедурам управления доступом, осуществлять оперативный контроль выполнения требований по обеспечению безопасности информации персоналом ИСПДн МЖКХиТЭК, участвовать в комиссии по расследованию инцидентов безопасности информации;
- осуществлять контроль текущего состояния защищенности ИСПДн МЖКХиТЭК;
- участвовать в рассмотрении технических заданий на проектирование, эскизных, технических и рабочих проектов, обеспечивать их соответствие действующим нормативным и методическим документам и эффективности

предлагаемых и реализуемых организационно-технических решений по защите информации;

- участвовать в проектах по созданию и совершенствованию системы защиты информации ИСПДн МЖКХиТЭК, разрабатывать предложения по выявлению и локализации возможных каналов утечки защищаемой информации, в том числе и в экстремальных (нештатных) ситуациях;
- принимать участие в работах, по тестированию внедряемых в ИСПДн МЖКХиТЭК новых информационных технологий;
- принимать участие в проведении ежегодного комплексного обследования состояния защищенности ИСПДн МЖКХиТЭК;
- осуществлять сбор материалов о состоянии мер и средств защиты информации в ИСПДн МЖКХиТЭК для подготовки предложений по совершенствованию защиты информации и эффективному использованию средств мониторинга и контроля;
- проводить периодический аудит выполнения требований и правил по защите информации, представленных в нормативной и организационно-распорядительной документации, осуществлять контроль использования пользователями и системными администраторами штатных средств защиты, входящих в состав операционных систем, систем управления базами данных и серверов приложений;
- проводить анализ журналов средств обнаружения вторжений на предмет выявления фактов сканирования сети, появления в сети незарегистрированных сетевых устройств, а также сетевых атак на ресурсы ИСПДн МЖКХиТЭК;
- проводить анализ журналов событий и лог-файлов оборудования ИСПДн МЖКХиТЭК, в частности серверных платформ системы управления базами данных (СУБД), серверов общего доступа, маршрутизаторов, коммутаторов;
- осуществлять удаленный контроль состояния программно-аппаратной среды автоматизированных рабочих мест персонала ИСПДн МЖКХиТЭК на соответствие требованиям к обеспечению информационной безопасности;
- при необходимости формировать ключевую информацию, распределять ее между пользователями систем и средств контроля подлинности (достоверности);

- проводить занятия с персоналом ИСПДн МЖКХиТЭК по вопросам обеспечения информационной безопасности, оказывать консультативную помощь персоналу ИСПДн МЖКХиТЭК по вопросам использования средств защиты информации;
- готовить ежемесячные отчеты о проделанной работе, принятых мерах по фактам нарушений требований политики информационной безопасности ИСПДн МЖКХиТЭК.

4.5. Обязанности системного администратора

Персонал ИСПДн МЖКХиТЭК с правами системного администратора отвечает за работоспособность программно-аппаратных платформ, включая установленное на них программное обеспечение (системные администраторы рабочих станций, серверов баз данных, серверов приложений, сетевого и иного технического оборудования, используемого в ИСПДн МЖКХиТЭК). На сотрудника с правами системного администратора возложено выполнение требований по защите информации в процессах обслуживания сопровождаемых ими информационных технологий.

Системный администратор (в объеме задач обеспечению защиты информации) обязан:

- управлять правами доступа пользователей к обслуживаемым системам, не допускать получения прав доступа неавторизованных в системе субъектов доступа, создавать учетные записи субъектов доступа только после выполнения всех требований по организации доступа к информационным ресурсам системы; своевременно информировать администратора безопасности о попытках нарушения правил доступа к ресурсам ИСПДн МЖКХиТЭК;
- поддерживать в работоспособном состоянии встроенные средства (функции) защиты, использовать встроенные средства регистрации событий, обнаружения ошибок и программных конфликтов;
- оперативно реагировать на события безопасности, прямо или косвенно связанные проявлениями угроз безопасности информации, ежедневно анализировать содержимое журналов событий и лог-файлов, информировать руководство о состоянии используемых средств защиты информации и мерах, необходимых для их улучшения;

- оказывать помощь в отражении атак и иных проявлений инцидентов безопасности, выявлении нарушителей и предоставлять информацию необходимую для проведения расследований по выявленным инцидентам и проблемам обеспечения безопасности информации;
- повышать свой профессиональный уровень в вопросах защиты информации;
- консультировать пользователей по правилам и требованиям к обеспечению безопасности информации в объеме сопровождаемых информационных технологий;
- участвовать в разработке инструкций и положений по обеспечению безопасности информации в сопровождаемых им информационных технологиях;
- контролировать работоспособность средств антивирусной защиты и проводить антивирусный контроль информационных ресурсов, расположенных в границах своей зоны ответственности;
- еженедельно выполнять резервное копирование конфигурационной и иной защищаемой информации, перечень которой установлен для ИСПДн МЖКХиТЭК;
- контролировать состояние программно-аппаратной среды (конфигурации) сопровождаемых систем на предмет выявления несанкционированных изменений в установленной технологии обработки, хранения и передачи информации.

Системному администратору категорически запрещается использовать свое служебное положение для просмотра пользовательских данных с целью удовлетворения своего любопытства.

По всем фактам выявленных нарушений требований к обеспечению мер защиты информации, также по фактам несанкционированных изменений в процессах функционирования обслуживаемых программных и программно-технических средств, системный администратор обязан сообщать непосредственному руководителю и администратору безопасности.

4.6. Обязанности сотрудников

Для каждого сотрудника с правами выделенной ему роли в ИСПДн МЖКХиТЭК в его зоне ответственности в должностных инструкциях должны быть регламентированы требования по обеспечению безопасности информации.

4.7. Обязанности сотрудников, наделенных правами приеме на работу и увольнения

При заключении трудового договора с новым сотрудником Министерства, полномочный представитель Министерства обязан убедиться, что в трудовом договоре (контракте) содержится требование по сохранению конфиденциальных сведений и выполнению требований режима безопасности и после того, как сотрудник будет уволен или изменит свое должностное положение.

Полномочный сотрудник, ответственный за выполнение кадровой работы, несёт ответственность за процесс прекращения занятости или изменение должностного состояния сотрудника и работает вместе с непосредственным руководителем увольняемого или перемещаемого по должностному назначению работника.

Должностное лицо, с вмененными ему обязанностями администратора безопасности ИСПДн МЖКХиТЭК, обязано довести до всех заинтересованных сторон из числа персонала ИСПДн МЖКХиТЭК об изменениях, связанных с его увольнением или перемещением.

Все сотрудники Министерства, уволенные или изменившие свое должностное положение, обязаны возвратить ранее выданные (выделенные) им ресурсы ИСПДн МЖКХиТЭК, находящиеся в их временном пользовании до прекращения ими деятельности в качестве полномочного субъекта доступа к ресурсам ИСПДн МЖКХиТЭК, в том числе:

- оборудование;
- программное обеспечение;
- программно-аппаратные средства;
- документы;
- иные ресурсы, выданные для работы.

4. УПРАВЛЕНИЕ ДОСТУПОМ

При назначении прав доступа и их регистрации в ИСПДн МЖКХиТЭК необходимо руководствоваться следующими правилами:

- каждому субъекту доступа должен быть присвоен уникальный идентификатор;
- субъект доступа должен быть зарегистрирован администратором безопасности;
- при регистрации субъекта доступа должна быть проведена проверка соответствия предоставляемого ему уровня доступа возложенным задачам (вмененным обязанностям);
- назначенные субъекту доступа права должны быть задокументированы;
- субъекты доступа знакомятся с предоставленными им правами и порядком их использования под роспись;
- системным администратором должен проводиться контроль и своевременное удаление неиспользуемых учетных записей;
- запасные (на случай нештатных ситуаций) идентификаторы субъектов доступа должны быть доступны только под правами администратора безопасности;
- каждой роли должны соответствовать минимально необходимые привилегии для выполнения субъектом доступа возложенных на него задач.
- привилегии доступа нельзя предоставлять, пока субъект доступа не прошел процедуру аутентификации;
- все процессы, которые выполняются без процедуры аутентификации (доступ по умолчанию) должны быть идентифицированы и контролироваться;
- привилегии доступа в соответствии с выделенной для субъекта доступа ролью должны персонифицироваться учетной записью пользователя (процесса).

5.1. Управление и контроль доступа

Роли субъектов доступа устанавливаются в соответствии с требованиями организационно-распорядительной документации на систему защиты персональных данных ИСПДн МЖКХиТЭК, а также с учетом требований производителей, используемых средств автоматизации процессов управления доступом.

Все субъекты доступа по целевым задачам, решаемым ими в ИСПДн МЖКХиТЭК, должны относиться к одной из групп: пользователи, операторы, администраторы и

аудиторы. Привилегии доступа к ресурсам ИСПДн МЖКХиТЭК для субъектов данных групп доступа не должны перекрываться.

Зарегистрированным в ИСПДн МЖКХиТЭК пользователям, в том числе из числа обслуживающего персонала, определяются ясные и однозначно интерпретируемые права доступа. Пользователи ИСПДн МЖКХиТЭК должны обладать минимально необходимыми привилегиями для выполнения поставленных задач в рамках конкретных технологических процессов (приложений). Не допускается наделение пользователей ИСПДн МЖКХиТЭК правами, дающими возможность отменять системный и/или прикладной процесс в ИСПДн МЖКХиТЭК.

Администраторы обладают максимальными привилегиями в рамках конкретных технологических процессов ИСПДн МЖКХиТЭК, при этом предоставление одной учетной записи администратора доступа к ресурсам нескольких несвязанных процедурами администрирования процессов должно быть максимально ограничено.

Привилегированные права доступа, позволяющие вносить изменения в процессы функционирования ИСПДн МЖКХиТЭК, включая изменения в конфигурации средств защиты информации, а также позволяющие получить контроль за их функционированием (мониторингом состояния) предоставляются только по указанию ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

Сотрудники, выполняющие в соответствии с функциональными обязанностями процедуры аудита и мониторинга состояния защищенности ИСПДн МЖКХиТЭК, обладают минимальными привилегиями (только просмотр, чтение), при этом для одной учетной записи аудитора может быть предоставлен доступ к максимально возможному числу систем и средств автоматизации, используемых в ИСПДн МЖКХиТЭК.

В границах представленных групп доступа может строиться иерархия подгрупп субъектов доступа по предоставленным им привилегиям, при этом условия, определяющие характер требований родительских групп не должны нарушаться.

Роль, закрепленная (выделенная для использования) за конкретным субъектом доступа (пользователем, процессом) считается персонифицированной.

5.2. Управление паролями

Для каждого субъекта доступа к ресурсам ИСПДн МЖКХиТЭК устанавливается пароль одного из следующих типов:

- административный;
- операторский;

- пользовательский.

Административный пароль – предназначен для реализации полного доступа к ресурсам соответствующей системы или средствам ИСПДн МЖКХиТЭК с правами изменения всех параметров конфигурации, предоставления субъектам доступа прав административного, операторского или пользовательского доступа.

Операторский пароль – предназначен для реализации ограниченного доступа к ресурсам соответствующей системы или средства ИСПДн МЖКХиТЭК с правами чтения всех параметров конфигурации и изменения только параметров, определенных эксплуатационными особенностями соответствующего программно-технического средства.

Пользовательский пароль – предназначен для доступа к ресурсам соответствующей системы или средства ИСПДн МЖКХиТЭК с правами минимально необходимыми для выполнения прикладных задач, в рамках функциональных обязанностей субъекта доступа.

Зарегистрированные в ИСПДн МЖКХиТЭК пользователи, включая обслуживающий персонал, должны быть ознакомлены с правилами использования паролей.

Управление паролями в ИСПДн МЖКХиТЭК включает следующие правила:

- ввод парольной информации должен быть защищен от возможного перехвата, как с использованием способов визуального наблюдения за действиями пользователя, так и при передаче пароля, в процессе аутентификации (авторизации) его по каналам связи и передачи данных;
- в случае удаленного получения пароля, регистрация пользователя осуществляется по временному паролю для установки защищенного соединения, а затем, после установления защищенного соединения, передается пользователю постоянный пароль;
- при получении пароля от администратора безопасности субъект доступа должен при первом входе выполнить смену пароля;
- в ИСПДн МЖКХиТЭК реализуется механизм контроля смены паролей субъектами доступа в соответствии с установленным периодом использования пароля;
- в случае нарушения пользователем сроков использования паролей, его учетная запись блокируется;

- временные пароли, используемые в ИСПДн МЖКХиТЭК выдаются пользователям безопасным способом, например, с использованием третьей доверенной стороны;
- запрещается хранить пароли доступа к ресурсам ИСПДн МЖКХиТЭК в незащищенном (незашифрованном) виде;
- заданные производителями по умолчанию пароли после инсталляции (установки) программно-аппаратных комплексов и/или программного обеспечения подлежат смене;
- запрещается разглашать пароли доступа к ресурсам ИСПДн МЖКХиТЭК;
- плановая смена паролей обслуживающего персонала проводится не реже одного раза в квартал;
- внеплановая смена паролей проводится в случае прекращения полномочий соответствующего субъекта доступа, либо в случае его компрометации;
- не реже 1 раза в год проводится выборочная проверка выполнения требований при формировании (генерации) паролей субъектов доступа.

5.3. Правила формирования пароля

Временные и постоянные пароли учетных записей пользователей должны быть уникальными и неповторяемыми, содержание не должно легко угадываться.

Пароли выбираются персоналом ИСПДн МЖКХиТЭК самостоятельно с учетом требований внутренних инструкций Министерства.

Каждый субъект доступа должен знать правила использования парольной информации. С должностными лицами из числа персонала, обслуживающего ИСПДн МЖКХиТЭК, ежеквартально должны проводиться занятия (инструктажи) по изучению требований парольной политики с последующей их подписью в журнале инструктажа.

5.4. Действия в случае компрометации пароля

Компрометацией пароля является обнаружение пароля в явном виде на бумажном носителе либо в электронном документе, установление факта хищения, утраты или передачи пароля другому лицу, а также факт работы под именем (логинем) авторизованного субъекта доступа в период его фактического отсутствия.

О случае компрометации пароля субъекта доступа должны быть немедленно извещены администратор безопасности и ответственный за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

Ответственным за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК и администратором безопасности предпринимаются меры по внеплановой смене пароля доступа.

В случае компрометации пароля субъекта доступа с правами администратора безопасности проводится смена паролей всех субъектов доступа, чьи пароли были сгенерированы централизованно под правами администратора безопасности.

5.5. Политика «чистого» стола и очистки экрана

На рабочих местах персонала ИСПДн МЖКХиТЭК, применяется политика «чистого стола» и очистки экрана, которая предполагает:

- хранение в сейфе или в запираемом шкафу неиспользуемой критичной для функционирования ИСПДн МЖКХиТЭК информации при отсутствии на рабочем месте ответственного за ее использование сотрудника;
- не оставление без присмотра компьютеров, терминалов и иного оборудования, обеспечивающего доступ к ресурсам ИСПДн МЖКХиТЭК, до выхода из системы (закрыт сеанс связи и используемых приложений, сервисов) и защиты рабочего стола компьютера экранной заставкой (или иным запорным механизмом), управляемой паролем или техническим средством аутентификации пользователя;
- запрет несанкционированного использования фотокопировальных устройств и других технологий репродуцирования (сканирующих устройств, цифровых камер);
- удаление остаточной информации из памяти принтеров и уничтожение бумажных копий документов, признанных не пригодными для дальнейшего использования.

5.6. Правила предоставления доступа к ресурсам ИСПДн МЖКХиТЭК

Для регистрации (создания учетной записи) субъекта доступа и предоставления ему (изменения) прав доступа к ресурсам ИСПДн МЖКХиТЭК руководитель сотрудника, которому необходима регистрация (изменения) подает заявку на имя ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

В заявке указывается:

- содержание запрашиваемых прав (регистрация нового субъекта доступа, расширение или сужение его полномочий и прав доступа к ресурсам ИСПДн МЖКХиТЭК ранее зарегистрированного субъекта);
- фамилия, имя и отчество заявителя, а также его должность;
- имя (логин) учетная запись, в случае изменений в ранее предоставленных правах доступа данного субъекта;
- цель (обоснование) для предоставления (изменения или лишения) прав доступа;
- перечень необходимые полномочия, которые необходимо предоставить, добавить или лишить с указанием ресурсов ИСПДн МЖКХиТЭК, к которым назначается (или отменяется) доступ. Наименование запрашиваемых ресурсов должно включать в себя: логическое имя средства обработки информации или информационного сервиса, сетевое имя и IP адрес средства обработки информации, перечень необходимых данных и их местоположение в системе.

Форма заявки на внесение изменений в списки пользователей приведена в Приложении 1.

На основании заявки, рассмотренной ответственным за обеспечение безопасности информации ИСПДн МЖКХиТЭК, администратор безопасности проверяет правомочность запрашиваемых полномочий, совместно с системным администратором запрашиваемых ресурсов производит необходимые действия по созданию (удалению) учетной записи субъекта доступа, присвоению ему пароля и заявленных прав доступа к ресурсам ИСПДн МЖКХиТЭК.

При необходимости администратор безопасности устанавливает на рабочую станцию субъекта доступа средства защиты информации, либо проводит контроль их наличия и соответствие режимов их работы требованиям по обеспечению безопасности информации.

Администратор безопасности проводит первичный аудит по принятым в ИСПДн МЖКХиТЭК мерам обеспечения информационной безопасности.

По окончании работ по предоставлению, изменению или лишению прав доступа к ресурсам ИСПДн МЖКХиТЭК администратор безопасности вносит изменения в матрицу(ы) доступа технических средств и информационных сервисов, которых коснулись выполненные им изменения.

Исполненные заявки хранятся в архиве администратора безопасности ИСПДн МЖКХиТЭК. Копии исполненных заявок могут также передаваться руководителям подразделений Министерства.

Хранение исполненных заявок должно обеспечивать возможность:

- восстановления полномочий субъектов доступа;
- контроля правомерности предоставленных субъектам доступа прав к тем или иным ресурсам ИСПДн МЖКХиТЭК при разборе конфликтных ситуаций;
- проверки (контроля) правильности настройки средств разграничения доступа.

Проверка прав субъектов доступа проводится администратором безопасности с периодичностью не реже 1 раза в месяц путем сравнения используемых субъектом прав доступа с правами доступа, представленными в матрице доступа проверяемого средства обработки информации или информационного сервиса.

5.7. Правила локального доступа к ресурсам

При выполнении работ по обслуживанию и сопровождению систем и средств обработки информации в ИСПДн МЖКХиТЭК обслуживающий персонал обязан соблюдать следующие правила локального доступа к рабочим станциям и серверам системы:

- сотрудники Министерства имеют право доступа к рабочим станциям и серверам системы только согласно своим служебным обязанностям;
- по окончании работы с информационными и иными ресурсами ИСПДн МЖКХиТЭК выполняется завершение всех открытых соединений с серверами системы;
- при уходе с рабочего места доступ к используемому оборудованию блокируется.

Сотрудникам Министерства запрещается:

- осуществлять сканирование и проводить попытки реализации атак сетевые ресурсы ИСПДн МЖКХиТЭК;
- сообщать кому-либо свои идентификаторы и пароли доступа в ИСПДн МЖКХиТЭК;
- устанавливать модемы и иные сетевые устройства без разрешения администратора безопасности;

- выключать (блокировать) программы-антивирусы и персональные межсетевые экраны на серверах и рабочих станциях без разрешения администратора безопасности;
- передавать кому-либо устройства двухфакторной аутентификации доступа к серверам и рабочим станциям;
- осуществлять доступ к серверам и рабочим станциям ИСПДн МЖКХиТЭК под правами других пользователей без разрешения администратора безопасности;
- осуществлять удаленный доступ к ресурсам ИСПДн МЖКХиТЭК в обход утвержденных правил доступа.

5.8. Правила удаленного доступа к ресурсам ИСПДн МЖКХиТЭК

При выполнении работ с использованием средств удаленного доступа полномочный сотрудник с правами доступа к ресурсам ИСПДн МЖКХиТЭК обязан соблюдать следующие правила:

- удаленный доступ к ресурсам ИСПДн МЖКХиТЭК осуществляется в соответствии с регламентированными правами доступа;
- рабочие станции, используемые для удаленного доступа к ресурсам ИСПДн МЖКХиТЭК, должны быть оборудованы сертифицированными по требованиям безопасности информации средствами межсетевого экранирования и криптозащиты каналов связи с ИСПДн МЖКХиТЭК, либо располагаться в сетевом сегменте, защищенном сертифицированным по требованиям безопасности информации межсетевым экраном, обеспечивающим кроме этого криптозащиту сетевого трафика в процессах удаленного взаимодействия с ресурсами ИСПДн МЖКХиТЭК;
- все субъекты удаленного доступа должны пройти процедуру предварительной регистрации, проверки их IP-адресов и получения персонального пароля доступа;
- доступ субъектов удаленного доступа осуществляется по полученному паролю после прохождения ими процедуры идентификации и аутентификации;
- субъекты удаленного доступа не должны иметь административные права доступа ко всем ресурсам ИСПДн МЖКХиТЭК;
- взаимодействие субъектов удаленного доступа в ходе выполнения процедур администрирования, обслуживания, технической поддержки и иных процедур

сопровождения СВТ ИСПДн МЖКХиТЭК должно осуществляться только по защищенным каналам связи с использованием VPN-технологии.

5.9. Правила формирования матрицы доступа к ресурсам ИСПДн МЖКХиТЭК

Необходимой и достаточной информацией для формирования матрицы доступа к ресурсам ИСПДн МЖКХиТЭК являются:

I. Атрибуты субъектов доступа, включающие в себя:

1. Вид доступа:

- административный доступ (А);
- операторский доступ (О);
- пользовательский доступ (Р);
- доступ контролера-аудитора¹⁰ (К).

2. Тип доступа:

- удаленный (R);
- локальный (L).

3. Авторизация (тип авторизации):

- с авторизацией (А);
- без авторизации (N).

4. Средства предоставления доступа (группа программных средств, применяемых для доступа к данным):

- системное программное обеспечение (S);
- программное обеспечение СУБД (В);
- прикладное программное обеспечение (Р);
- специальное (специализированное) программное обеспечение (Е).

II. Параметры прав доступа к обрабатываемым данным:

1. К данным и приложениям на уровне системного программного обеспечения:

- полный доступ (F);
- чтение (R);
- запись (W);
- удаление (D);
- выполнение\получение доступа (Е);
- обзор содержимого папки (L);
- особые разрешения (М).

¹⁰ Контролер-аудитор относится к особой категории субъектов доступа с правами пользователя ко всем системам и средствам ИСПДн МСЖКХ, что необходимо с целью контроля реализации регламентированных мер по обеспечению защиты информации в ИСПДн МСЖКХ.

2. К данным и приложениям на уровне программного обеспечения СУБД:
 - абсолютные права доступа (F);
 - чтение (R);
 - запись (W);
 - удаление (D).
 - выполнение\получение доступа (E)
 - особые разрешения (M).
3. К данным и приложениям на уровне прикладного программного обеспечения:
 - абсолютные права доступа (F);
 - чтение (R);
 - запись (W);
 - удаление (D);
 - выполнение\получение доступа (E);
 - особые разрешения (M).
4. К данным и приложениям на уровне специального (специализированного) программного обеспечения:
 - полный доступ (F);
 - чтение (R);
 - запись (W);
 - удаление (D);
 - выполнение\получение доступа (E);
 - обзор содержимого папки (L);
 - особые разрешения (M).

Модель правил предоставления прав доступа, в соответствии с которой формируется матрица доступа к ресурсам ИСПДн МЖКХиТЭК, представлена в таблице 1.

Пример матрицы доступа:

| № | Категория/должность субъекта доступа | Учетная запись | Атрибуты\права доступа | | |
|---|--------------------------------------|----------------|-------------------------------|--------------|-------------------------------|
| | | | APM-I | APM-T | APM-K |
| 1 | Системный администратор | root | ARAS\F-----M | ARAS\F-----M | ARAS\F-----M |
| 2 | Анонимный пользователь | anonymous | PRNP\ -R--E-, PRNB\ -R---- | - | PRNP\ -R--E-, PRNB\ -R---- |

Таблица 1. Модель правил предоставления доступа к ресурсам ИСПДн МЖКХиТЭК

[illegible]

5.10. Контроль обработки конфиденциальной информации

В целях выявления скрытых каналов утечки информации в ИСПДн МЖКХиТЭК и предпосылок к их созданию в процессе мониторинга и контроля защитных мер выполняется контроль используемых субъектами доступа данных.

Контроль используемых субъектами доступа данных включает в себя проверку содержания данных с целью выявления нарушений конфиденциальности информации. В качестве основных объектов контроля выступают хранилища с данными зарегистрированных пользователей, а также служебная и аутентификационная информация обслуживающего персонала.

Контроль доступа к данным, используемых в своей работе зарегистрированными пользователями и обслуживающим персоналом, проводится как для данных, расположенных на носителях (например, на жестких магнитных дисках), так и для данных, передаваемых по сети.

5. АНТИВИРУСНАЯ ЗАЩИТА

6.1. Общие требования к антивирусной защите

В целях предотвращения проявлений вредоносного кода в ИСПДн МЖКХиТЭК используются только официально приобретенные средства антивирусной защиты

Установка и регулярное обновление средств антивирусной защиты на серверах и рабочих станциях персонала осуществляться под правами учетной записи администратора безопасности ИСПДн МЖКХиТЭК. Отключение или не обновление антивирусных средств защиты не допускается. Запрещается установка на программно-аппаратные платформы ИСПДн МЖКХиТЭК, средств антивирусной защиты, не связанных с выполнением конкретных функций защиты.

При наличии серверных программно-аппаратных платформ установка обновлений антивирусных баз и используемого антивирусного программного обеспечения осуществляется в ручном режиме.

Устанавливаемое или изменяемое программное обеспечение ИСПДн МЖКХиТЭК должно быть предварительно проверено на отсутствие вирусов. После установки или обновления программного обеспечения в обязательном порядке выполняется антивирусная проверка.

Установка и обновление антивирусных средств защиты контролируется администратором безопасности.

Средства антивирусной защиты должны обеспечивать проверку:

- любых файлов на электронных или оптических носителях;
- файлов и данных, полученных по сети;
- вложений в письма электронной почты;
- контента автоматизированных рабочих мест и серверов ИСПДн МЖКХиТЭК.

Ответственность за проведение антивирусной проверки серверов и рабочих станций возлагается на системного администратора, в зону ответственности которого входит администрирование программно-аппаратных платформ ИСПДн МЖКХиТЭК.

6.2. Правила применения средств антивирусной защиты

Ежедневно перед началом работы после загрузки операционных систем на рабочих станциях персонала ИСПДн МЖКХиТЭК в автоматическом режиме должен проводиться антивирусный контроль всех используемых для работы носителей информации (дисков и

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
файлов). Антивирусный контроль при наличии серверов в ИСПДн МЖКХиТЭК выполняется еженедельно.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

Антивирусный контроль входящей (получаемой) информации проводится непосредственно после ее приема (получения). В случае получения информации из недостоверных источников, расположенных во внешних информационных системах, антивирусный контроль осуществляется на специально выделенном сервере (сервер доступа к ресурсам сети Интернет).

Антивирусный контроль исходящей (передаваемой) информации проводится непосредственно перед архивированием и отправкой.

Проведение антивирусного контроля обязательно при выполнении работ по установке (обновлении) системного и/или прикладного программного обеспечения, используемого в ИСПДн МЖКХиТЭК.

6.3. Требования к процессам функционирования подсистемы антивирусной защиты

В процессах функционирования подсистемы антивирусной защиты должны выполняться следующие требования:

- регламентирован порядок безопасного получения файлов данных и программного обеспечения, устанавливающий какие защитные меры должны выполняться и какие средства защиты использоваться;
- определен плановый антивирусный контроль используемого программного обеспечения и данных;
- применяемые средства антивирусной защиты обеспечивают детектирование, лечение и удаление вредоносного кода, а также установку обновлений антивирусных баз;
- определены обязанности персонала, в части выполнения мер защиты от вредоносного кода, организовано его обучение, определен порядок оповещения о вирусных атаках, а также установлены меры по локализации вредоносного кода;
- осуществляется регулярный сбор информации относительно новых разновидностей видов и форм вредоносного кода.

6. ИСПОЛЬЗОВАНИЕ НЕКОНТРОЛИРУЕМЫХ РЕСУРСОВ СЕТИ ИНТЕРНЕТ

7.1. Общие требования к организации доступа к сети Интернет

Доступ к неконтролируемым информационным ресурсам¹¹ сети Интернет в ИСПДн МЖКХиТЭК осуществляется в двух режимах: on-line и off-line.

Подключение в режиме on-line осуществляется путем установления непосредственного соединения с web- и иными серверами, расположенными в сети Интернет.

Использование неконтролируемых ресурсов сети Интернет в режиме on-line допускается только в ходе проведения работ по техническому обслуживанию программных и программно-технических средств ИСПДн МЖКХиТЭК. В иных случаях доступ к неконтролируемым информационным ресурсам сети Интернет в режиме on-line запрещен.

В случае предоставления доступа в режиме on-line необходимость его должна быть обоснована требованиями технологических процессов ИСПДн МЖКХиТЭК. Подключение оборудования (серверов и рабочих станций) ИСПДн МЖКХиТЭК к сети Интернет в режиме off-line осуществляется только с использованием специально выделенного сервера доступа к ресурсам сети Интернет (проxy сервера), расположенного в границах демилитаризованной зоны ИСПДн МЖКХиТЭК. На данном сервере разворачивается клиентское программное обеспечение, средства антивирусной защиты, защиты от несанкционированного доступа, контроля целостности, а также программы просмотра исходного кода программного обеспечения, содержания web контента, чтения и просмотра текстовых и иных файлов, включая файлы с медиа-контентом.

Для наиболее критичных компонентов ИСПДн МЖКХиТЭК, таких как серверы хранения персональных данных и иной конфиденциальной информации, файловые и иные информационные массивы, для которых не предусмотрены процедуры хранения резервных копий, осуществляться проверка на отсутствие программных конфликтов путем размещения запрошенного информационного ресурса в программно-аппаратную среду, эмулирующую потенциальный объект размещения запрошенного информационного ресурса.

¹¹ В данном контексте под неконтролируемыми ресурсами понимаются информационные ресурсы web и иных серверов, расположенных в сети Интернет, доступ к которым не регламентирован установленным порядком и правилам информационного взаимодействия ИСПДн МСЖКХ с внешними информационными системами.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Все факты подключения и получения из сети Интернет неконтролируемых информационных ресурсов должны регистрироваться администратором безопасности.

Запрещается перенос информации (технической документации, исполняемых модулей, программ, драйверов, информационных материалов и т.п.) на другое оборудование ИСПДн МЖКХиТЭК без санкции администратора безопасности. В случае нарушения установленного порядка и правил использования информационных ресурсов сети Интернет администратор безопасности вправе блокировать действия нарушителя и принять меры реагирования по факту выявленного инцидента безопасности.

7.2. Порядок получения доступа в режиме on-line

Получение доступа к неконтролируемым информационным ресурсам сети Интернет в режиме on-line осуществляется в следующем порядке:

- уполномоченный системный администратор направляет согласованный с администратором безопасности запрос (служебную записку) ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК с указанием: режима подключения, тематики или адресной информации запрашиваемого информационного ресурса, цель подключения и время, необходимое для его получения;
- на основании решения ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК, уполномоченный системный администратор выполняет подключение к сети Интернет, скачивает информационный ресурс, выполняет его антивирусный контроль, проверяет его содержание на соответствие требованиям технологического процесса, для которого данный ресурс был востребован и использует ресурс по назначению;
- по окончании использования информационного ресурса, уполномоченный системный администратор информирует администратора безопасности и регистрирует факт в Журнале технического обслуживания соответствующего оборудования ИСПДн МЖКХиТЭК (см. Приложение 2).

7.3. Порядок получения доступа в режиме off-line

Получение доступа к неконтролируемым информационным ресурсам сети Интернет в режиме off-line осуществляется в следующем порядке:

- уполномоченный системный администратор направляет согласованный с администратором безопасности запрос (служебную записку) ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК с

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

указанием: режима подключения, тематики или адресной информации запрашиваемого информационного ресурса, цель подключения и время, необходимое для его получения;

- на основании решения ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК администратор безопасности выполняет подключение к сети Интернет, используя сервер доступа к ресурсам Интернет, скачивает запрашиваемый информационный ресурс, выполняет антивирусный контроль, контроль целостности, идентифицирует состав и содержание полученного ресурса, а при необходимости эмулирует программно-аппаратную среду оборудования, на котором предполагается установка (размещение) полученного ресурса, и проводит проверку на отсутствие программных конфликтов;
- в случае положительного заключения по результатам проведенных проверок, администратор безопасности передает полученный из сети Интернет информационный ресурс уполномоченному системному администратору для использования в ИСПДн МЖКХиТЭК;
- по окончании использования полученного ресурса системный администратор информирует администратора безопасности и регистрирует факт завершения работы в Журнале технического обслуживания соответствующего оборудования ИСПДн МЖКХиТЭК.

7. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ СЕТЕВЫХ РЕСУРСОВ

8.1. Общие требования по обеспечению безопасности сетевых ресурсов

Применяемые в ИСПДн МЖКХиТЭК меры сетевой защиты должны обеспечивать решение задач:

- идентификации сетевых ресурсов ЛВС ИСПДн МЖКХиТЭК, ассоциирование их с сетевыми именами и адресами.
- защиту сетевых информационных ресурсов, расположенных на СВТ ИСПДн МЖКХиТЭК, от угроз несанкционированного удаленного доступа.
- активный динамический контроль использования сетевых ресурсов ИСПДн МЖКХиТЭК.
- обнаружение сетевых атак на сетевые ресурсы.

Сетевая инфраструктура ЛВС ИСПДн МЖКХиТЭК включает в себя три домена безопасности:

- домен безопасности «Бухгалтерский архив», в состав которого входят сетевой сегмент, в границах которых расположены СВТ, предназначенные для обработки персональных данных в процессах ведения бухгалтерского архива;
- домен безопасности «Строительство и ЖКХ» предназначенные для обработки персональных данных в процессах выполнения государственных и региональных задач, возложенных на Министерство, в состав которого входят все сетевые сегменты с АРМ персонала ИСПДн МЖКХиТЭК, включая СВТ домена безопасности «Бухгалтерский архив»;
- домен безопасности «ДМЗ12» (демилитаризованная зона), в состав которого входят СВТ, расположенные в сетевом сегменте ЛВС ИСПДн МЖКХиТЭК, предназначенные для доступа к расположенным на них информационным ресурсам из внешних информационных систем.

Защита сетевых ресурсов ИСПДн МЖКХиТЭК построена как двухэшелонная сетевая защита СВТ, предназначенных для обработки и хранения персональных данных и иной подлежащей защите информации.

Первый эшелон сетевой защиты строиться с использованием средств межсетевого экранирования, расположенных на границе сетевого периметра ЛВС ИСПДн

¹² ДМЗ - демилитаризованная зона

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
МЖКХиТЭК. Для этого применяются сертифицированный межсетевой экран/криптошлюз с функциями фильтрации сетевого трафика на 3-е и 4-ом уровнях по модели OSI.

Второй эшелон сетевой защиты строиться с использованием средства межсетевого экранирования, выступающего в качестве центрального маршрутизатора, обеспечивающего защищенное взаимодействие между сетевыми сегментами доменов безопасности ИСПДн МЖКХиТЭК.

Базовым требованием к сетевой защиты ИСПДн МЖКХиТЭК является: «Доступ из внешних сетей к СВТ ИСПДн МЖКХиТЭК без использования сертифицированных средств межсетевого экранирования и криптографической защиты сетевого трафика запрещен». Все попытки получения доступа из внешних информационных сетей (в частности из сети Интернет) должны блокироваться.

Для минимизации вероятности проявления угроз: нарушения целостности процессов информационного обмена, а также нарушений доступности программных серверов, сетевых служб и сервисов, в ИСПДн МЖКХиТЭК должна применяться технологии «горячего», либо «холодного» резервирования средств межсетевого экранирования.

8.2. Организация сетевой защиты ЛВС ИСПДн МЖКХиТЭК

Применяемые в ИСПДн МЖКХиТЭК меры сетевой защиты должны гарантировать то, что персональные данные и иная информация конфиденциального характера, обрабатываемая в ИСПДн МЖКХиТЭК, попадет по назначению и не будет перехвачена, модифицирована или блокирована.

Кроме этого, меры сетевой защиты не должны ухудшать основные процессы функционирования ИСПДн МЖКХиТЭК, в частности снижать требования к обеспечению их непрерывности.

В ЛВС ИСПДн МЖКХиТЭК может применяться технология VLAN - виртуальных локальных сетей. Технология VLAN обеспечивает возможность коммутации пакетов на уровне коммутаторов уровня доступа и/или распределения. Безопасность от вторжения извне обеспечивается путем применения функции фильтрации протоколов, а также функции сетевой безопасности на уровне доступа к портам коммутаторов за счет применения списков контроля доступа - (Access Control List) и функции аутентификации принадлежности обрабатываемых пакетов к определенному VLAN.

Функции фильтрации протоколов уровня L2 обеспечивается коммутаторами второго уровня. Фильтрация протоколов заключается в передаче трафика указанного протокола с одновременной обработкой его через заданный порт.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Функция обеспечения безопасности на уровне портов коммутатора позволяют настроить какой-либо порт так, чтобы доступ к коммутатору через этот порт предоставлялся только заданному устройству или группе устройствам.

Списки контроля доступа, применяемые на маршрутизаторах и межсетевых экранах ИСПДн МЖКХиТЭК, используют для фильтрации сетевого трафика адресную информацию об отправителе и получателе данных, а также сведения о TCP/UDP портах, и определяют, каким образом сетевой трафик обрабатывается на конкретном маршрутизаторе или межсетевом экране.

Списки контроля доступа на маршрутизаторах внутреннего домена безопасности должны ограничивать доступ от и к СВТ данного домена только необходимыми для функционирования ИСПДн МЖКХиТЭК IP-адресами, портами и протоколами.

Комплексное применение в ИСПДн МЖКХиТЭК маршрутизаторов, межсетевых экранов и коммутаторов обеспечивает сетевую защиту от угроз:

1. Неавторизованного доступа – обнаруживается средством обнаружения вторжений и нейтрализуется фильтрацией на межсетевом экране или маршрутизаторе с функциями фильтрации сетевого трафика.
2. Атак уровня приложений – обнаруживается средством обнаружения вторжений и нейтрализуется фильтрацией на межсетевом экране.
3. Подбора паролей (парольные атаки) - ограничиваются сокращением количество попыток получения доступа.
4. Отказ в обслуживании - обнаруживается средством обнаружения вторжений и нейтрализуется ограничением скорости доступа на границе ЛВС ИСПДн МЖКХиТЭК с сетью оператора связи, а также настройкой контроля TCP-соединений на межсетевом экране.
5. Злоупотребления доверием – возможностью злоупотребления доверием ограничивается использованием приемов сегментации сетевых ресурсов ЛВС ИСПДн МЖКХиТЭК, а также созданием виртуальных локальных сетей (VLAN), что позволяет предотвратить ненужное взаимодействие СВТ внутри сети.
6. Переадресации портов – ограничивается применением запретительной фильтрации.

8.3. Защита каналов связи

Меры защиты информации, передаваемой через открытые каналы связи с внешними информационными системами, включают в себя:

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- управление доступом к ресурсам межсетевого обмена;
- идентификацию и аутентификацию абонентов сетевого доступа (включая криптографические способы аутентификации);
- идентификацию и аутентификацию передаваемой информации;
- криптографическую защиту информации в каналах связи, выходящих за границу контролируемой зоны ИСПДн МЖКХиТЭК;
- криптографическую изоляцию взаимодействующих систем.

В качестве основных средств защиты информации, передаваемой по открытым каналам связи, применяются программно-аппаратные комплексы (крипто-шлюзы), обеспечивающие реализацию методов криптографической защиты в соответствии с технологией виртуальных частных сетей (VPN) как при взаимодействии с внешними информационными системами, так и в процессах организации удаленного доступа обслуживающего административно-технического персонала ИСПДн МЖКХиТЭК.

Порядок применения СКЗИ в ИСПДн МЖКХиТЭК включает в себя:

- порядок ввода в действие;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой системой;
- порядок обращения с носителями ключевой информации.

Применение СКЗИ в ИСПДн МЖКХиТЭК должно обеспечиваться протоколированием работы СКЗИ и контролем целостности используемого программного обеспечения.

Безопасность процессов изготовления ключевых документов в ИСПДн МЖКХиТЭК обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

Применяемые в ИСПДн МЖКХиТЭК СКЗИ должны соответствовать следующим требованиям:

- СКЗИ обеспечивают функции шифрования на основе алгоритмов, соответствующих национальным стандартам Российской Федерации;
- зашифрованное сообщение может быть прочитано только при наличии ключа шифрования;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей. В среднем при лобовой атаке криптоаналитику необходимо перебрать половину всех возможных ключей, но в наихудшем случае ему придется перебрать все ключи;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей имеет строгую нижнюю оценку и выходит за пределы возможностей современных компьютеров (с учетом возможности использования распределенных вычислений);
- знание алгоритма шифрования не влияет на надежность защиты (принцип Кирхгофа);
- незначительное изменение ключа приводит к существенному изменению вида зашифрованного сообщения – так называемый принцип распространения ошибки;
- структурные элементы алгоритма шифрования должны быть неизменными, т.е. должен быть реализован их контроль целостности;
- дополнительные биты, вводимые в сообщение в процессе шифрования, (например, при дополнении открытого текста до длины, кратной длине блока алгоритма шифрования) полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста равной длине открытого текста;
- отсутствуют легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных обеспечивает надежную защиту информации, т.е. из ключевого множества исключены заведомо слабые ключи.

Для обеспечения поддержки используемых в ИСПДн МЖКХиТЭК СКЗИ регламентированы следующие требования:

- доступ к работе со СКЗИ только на основании приказа Министерства;
- применяемые в ИСПДн МЖКХиТЭК СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- принятый к исполнению регламент использования ключей, должен обеспечивать контроль со стороны администратора безопасности за

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

действиями пользователя СКЗИ на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);

- должна обеспечивать реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей или при переходе системы (комплекса) в нештатный режим работы;
- организация использования СКЗИ не должна содержать требований по специальной проверке СВТ ИСПДн МЖКХиТЭК на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;
- организация использования СКЗИ в ИСПДн МЖКХиТЭК не должно требовать дополнительной защиты от утечки по побочным каналам электромагнитного излучения.

Обязательным условием организации работы со СКЗИ является ведение Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов и Журнала учета мероприятий по техническому обслуживанию средств защиты информации.

8.4. Безопасность сетевых служб

Безопасность сетевых служб определяется требованиями к обеспечению непрерывности сетевого доступа к информационным сервисам ИСПДн МЖКХиТЭК, а также требованиями к управлению сетевыми службами, которые должны быть идентифицированы и включены в соглашение о сетевых услугах, заключенного с организацией-провайдером услуг связи с внешними информационными системами.

В ИСПДн МЖКХиТЭК должны регулярно контролироваться условия предоставления сетевых сервисов, а в случае использования услуг, предоставляемых третьей стороной (провайдером), его квалификация. Обязательным требованием контроля уровня предоставляемого сетевого сервиса является право на аудит услуг, предоставляемых провайдером.

При использовании специфических служб, таких как защита каналов связи, удаленное администрирование, обслуживание сетевых ресурсов внешней по отношению к Министерству организацией, необходимо обеспечить выполнение двусторонних соглашений в рамках отдельных договоров о предоставлении целевого сервиса, при этом внешняя сторона должна документально подтвердить заявленные ей гарантии и меру

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

ответственность в случае их нарушений. Службы сетевого сервиса должны включать в себя обеспечение устойчивого канала связи, поддержку мультисервисных услуг, служб поддержки виртуальной частной сети, администрирования сетевых служб DHCP, DNS, WINS и т.д., управляемых сетевых решений по защите информации (типа систем межсетевых экранов и/или систем обнаружения вторжений). Предоставляемые услуги могут ранжироваться, от предоставления простой неконтролируемой полосы пропускания до сложных биллинговых решений, обеспечивающих динамическое поддержание полосы пропускания для определенного сетевого сервиса.

Решения по защите сетевых служб должны учитывать:

- применяемые технологии удаленного доступа к сетевым ресурсам ИСПДн МЖКХиТЭК, в частности технологии идентификации, авторизации, кодирования и мониторинга сетевых подключений;
- технологии безопасного использования сетевых служб в соответствии с параметрами встроенных в них механизмов защиты и правил межсетевого доступа;
- процедуры и регламенты работы конкретной сетевой службы, в которых должны быть четко и понятно определены права и ответственность за качество предоставляемых услуг, а также определены порядок, права доступа и перечень разрешенных операций.

8. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ

Контроль состояния защищенности ИСПДн МЖКХиТЭК организуется и проводится в целях определения истинного состояния защищенности ИСПДн МЖКХиТЭК, оценки эффективности принимаемых мер защиты, выявления возможных каналов утечки защищаемых сведений, выработки предложений и рекомендаций по совершенствованию системы защиты персональных данных.

Структура процессов контроля состояния защищенности ИСПДн МЖКХиТЭК определяется в виде групп процессов: группа процессов контроля текущего состояния защищенности используемых в ИСПДн МЖКХиТЭК систем и средств обработки, хранения и передачи информации и группа процессов комплексного обследования состояния защищенности ИСПДн МЖКХиТЭК. Обе группы процессов контроля состояния защищенности ИСПДн МЖКХиТЭК имеют свои особенности и взаимно дополняют друг друга.

Существенной особенностью контроля текущего состояния защищенности ИСПДн МЖКХиТЭК является тот факт, что контроль текущего состояния защищенности осуществляется непрерывно в отличие от комплексного обследования состояния защищенности, которое проводится не реже одного раза в год, либо по приказу (распоряжению) Министерства.

9.1. Контроль текущего состояния защищенности ИСПДн МЖКХиТЭК

Выполнение процедур контроля текущего состояния защищенности ИСПДн МЖКХиТЭК возлагается на администратора безопасности.

Основными задачами администратора безопасности по контролю текущего состояния защищенности ИСПДн МЖКХиТЭК являются:

- сбор, обобщение и анализ конфигураций, применяемых в ИСПДн МЖКХиТЭК систем и средств защиты информации;
- анализ состояния процессов управления, администрирования, сопровождения, технической поддержке, обслуживания СБТ, обработки, хранения, передачи и защиты информации на предмет выявления несанкционированных изменений и нарушений установленного регламента;
- проведение контроля целостности программного обеспечения, критичного для функционирования ИСПДн МЖКХиТЭК, в том числе архивов баз данных, копий дистрибутивов и конфигураций программного обеспечения;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- обработка и анализ событий безопасности, выявление критичных событий, инициирование процедур ответной реакции (реагирования) по фактам выявленных нарушений и иных проявлений угроз безопасности информации;
- проведение выборочного контроля соблюдения административно-техническим персоналом ИСПДн МЖКХиТЭК требований документов политики информационной безопасности, в частности порядка и правил предоставления доступа к ресурсам ИСПДн МЖКХиТЭК;
- проверка выполнения административно-техническим персоналом требований по работе съемными носителями информации;
- поиск и анализ уязвимостей программного обеспечения, инициирование процедур управления релизами;
- разработка и предоставление руководству отчетных материалов с результатами оценки текущего состояния защищенности ИСПДн МЖКХиТЭК.

Проведенные мероприятия по контролю состояния защищенности ИСПДн МЖКХиТЭК регистрируются в журнале контроля выполнения требований, предъявляемых к обеспечению безопасности персональных данных (см. Приложение 2).

В качестве инструментальных (программно-технических) средств контроля состояния защищенности ИСПДн МЖКХиТЭК администратор безопасности должен использовать:

- средства мониторинга событий;
- средства контроля доступа (аутентификации) в среду функционирования системного и прикладного программного обеспечения;
- средства защиты информации от НСД, антивирусной защиты, межсетевого экранирования и криптозащиты сетевого трафика с функциями регистрации событий;
- средства контроля целостности программного обеспечения и данных;
- средства обнаружения уязвимостей.

9.2. Комплексное обследование состояния защищенности ИСПДн МЖКХиТЭК

Алгоритм подготовки и проведения комплексного обследования состояния защищенности ИСПДн МЖКХиТЭК включает в себя:

- определение цели и принятие решения о проведении обследования;
- подготовка перечней проверяемых вопросов;
- определение и назначение проверочной комиссии;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- определение сроков работы комиссии;
- разработка и утверждение плана проведения обследования;
- проведение работ по комплексному обследованию защищенности ИСПДн МЖКХиТЭК;
- оформление отчета по результатам выполненных работ;
- разработка предложений и рекомендаций по совершенствованию системы защиты информации;
- предоставление результатов обследования руководству.

Проведение работ по комплексному обследованию защищенности ИСПДн МЖКХиТЭК включают в себя:

- анализ полноты и достаточности организационно-распорядительных документов;
- проведение обследования на местах (на средствах обработки, хранения, передачи и обеспечения защиты информации).

В ходе проведения комплексного обследования оцениваются следующие базовые показатели состояния защищенности ИСПДн МЖКХиТЭК:

- оценка актуальности результатов моделирования угроз безопасности информации;
- оценка полноты и достаточности организационно-распорядительных документов политики информационной безопасности ИСПДн МЖКХиТЭК;
- оценка процессов управления процедурами назначения и распределения ролей, а также обеспечения уровня доверия к персоналу ИСПДн МЖКХиТЭК;
- оценка мер обеспечения безопасности информации в процессах функционирования технических и программно-технических средств и систем обработки, хранения и передачи информации;
- оценка мониторинга и контроля защитных мер по регистрации действий и событий безопасности;
- оценка процессов управления доступом и регистрации событий;
- оценка мер по обнаружению вторжений и реагированию на инциденты безопасности информации;
- оценка мер обеспечения антивирусной защиты;
- оценка мер обеспечения безопасности информации в процессах взаимодействия с внешними информационными системами;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- оценка мер обеспечения безопасности информации средствами криптографической защиты информации;
- оценка выполнения программ обучения и уровня осведомленности персонала ИСПДн МЖКХиТЭК по вопросам защиты информации.

Особый вид проверок – контрольные проверки состояния защищенности ИСПДн МЖКХиТЭК.

Как правило, данный вид контроля является следствием реакции руководства Министерства на инциденты безопасности информации либо для получения руководством свидетельств того, что ранее принятые решения по совершенствованию системы защиты персональных данных в ИСПДн МЖКХиТЭК выполнены.

9.3. Обнаружение вторжений в процессы функционирования ИСПДн МЖКХиТЭК

Обнаружение вторжений – это процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные или сетевые ресурсы ИСПДн МЖКХиТЭК.

Обнаружение вторжений в процессы функционирования ИСПДн МЖКХиТЭК является частью процессов контроля текущего состояния защищенности, целью которых является выявление атакующих источников угроз, прошедших применяемые в ИСПДн МЖКХиТЭК превентивные меры и средства защиты.

Основными средствами обнаружения вторжений в ИСПДн МЖКХиТЭК являются:

- средства контроля целостности конфигураций программных и программно-технических средств обработки, хранения, передачи и защиты информации;
- средства регистрации и контроля использования учетных записей субъектов доступа;
- средства антивирусной защиты;
- встроенные в системное и прикладное программное обеспечение средства контроля доступа субъектов, регистрирующих нарушения правил идентификации и аутентификации субъектов доступа;
- средства обнаружения уязвимостей в программном обеспечении
- средства контроля адресного пространства ЛВС ИСПДн МЖКХиТЭК, используемых TCP/UDP портов сетевых приложений;
- средства обнаружения вторжений и сетевых атак, использующих сигнатурные и эвристические методы контроля сетевого трафика;
- средства межсетевого экранирования с функциями выявления аномалий в сетевых протоколах прикладного уровня.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Распределение обязанностей персонала ИСПДн МЖКХиТЭК в процессах обнаружения вторжений определяется предоставленными правами доступа к средствам обработки, хранения, передачи и защиты информации.

9. ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

10.1. Общие требования к использованию мобильных технических средств

В качестве мобильных технических средств в ИСПДн МЖКХиТЭК разрешается использование съемных машинных носителей информации типа: флэш-накопители, внешние накопители на жестких дисках и иные пассивные устройства хранения данных.

Использование мобильных (портативных) вычислительных устройств типа ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные устройства в ИСПДн МЖКХиТЭК, а также иных мобильных технических средств со встроенными микропроцессорными системами (компонентами), запрещено.

Меры по обеспечению безопасности обрабатываемых в ИСПДн МЖКХиТЭК персональных данных и иной защищаемой информации при использовании мобильных технических средств типа съемных машинных носителей информации (далее – съемные носители информации), разрешенных к использованию, включают в себя:

- регламентацию и выполнение правил использования, учета, хранение, передачи и уничтожение съемных машинных носителей, разрешенных к использованию;
- запрет использования неучтенных съемных машинных носителей информации, разрешенных к использованию;
- запрет возможности автозапуска программного обеспечения (программного кода), находящегося на съемных машинных носителях информации, разрешенных к использованию;
- ограничение на использование съемных машинных носителей информации, разрешенных к использованию, в соответствии с производственной необходимостью.

10.2. Организация учета съемных носителей информации

Учету подлежат все съемные машинные носители информации. Для учета съемные машинные носители информации администратором безопасности ведется журнал учета съемных машинных носителей информации (см. Приложение 2).

Учётный номер носителя состоит из сокращенного наименования подразделения (отдела) и порядкового номера по журналу регистрации через дефис

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
(например, уч. № ОБ-1/К, где ОБ – отдел бухгалтерии, 1 – порядковый номер в журнале, К – «Конфиденциально»).

В случае отсутствия утвержденных сокращений названий подразделений учетный номер носителя состоит из порядкового номера по журналу регистрации (например, уч. № 01/К, где 01 – порядковый номер в журнале, К – «Конфиденциально»).

Номер наносится непосредственно на съемный машинный носитель информации (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяются другие доступные способы маркировки.

Накопители на жестких магнитных и твердотельных дисках, размещенные в системных блоках СВТ учитываются в техническом паспорте (формуляре) на поставляемое оборудование с указанием марки носителя информации и его серийного номера.

Ответственным за организацию учета мобильных технических средств является администратор безопасности.

10.3. Организация хранения и выдачи съемных носителей информации

Съемные машинные носители информации должны храниться в надежно запираемых хранилищах, учет которых ведет администратор безопасности в журнале учета мест хранения съемных машинных носителей информации (см. Приложение 2). Ко всем хранилищам необходимо иметь по два экземпляра ключей. Один из экземпляров ключей находится у полномочного сотрудника, запасной экземпляр хранится у руководителя структурного подразделения.

О фактах утраты носителей необходимо незамедлительно докладывать администратору безопасности и руководителю структурного подразделения.

Выдача съемных машинных носителей информации осуществляется администратором безопасности под подпись с отметкой в журнале учета съемных машинных носителей информации. Факт сдачи носителя регистрируется аналогичным образом. Передача съемных машинных носителей третьим лицам запрещена.

10.4. Организация уничтожения съемных носителей информации

Уничтожение съемных носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления. Перед уничтожением вся информация с него должна быть стерта (уничтожена).

Уничтожение информации на съемных машинных носителях информации производится с использованием специальных средств (программные или программно-

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путем полного трехкратного его форматирования. Для контроля невозможности восстановления уничтоженной информации необходимо применять сертифицированные средства контроля удаления информации.

Уничтожение носителей, затирание (уничтожение) информации со съемных машинных носителей информации производится постоянно действующей комиссией по уничтожению, назначенной приказом Министерства

По факту уничтожения носителей комиссией составляется акт. В акте указываются учетные номера носителей, характер уничтожаемой (затираемой) информации, причина уничтожения носителя (затирания информации на нем). Форма акта представлена в Положении об учёте, хранении и использовании съемных носителей, предназначенных для хранения и передачи персональных данных Приложении 1.

Реквизиты акта заносятся администратором безопасности в журнал учета съемных машинных носителей информации. Акт хранится у ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

10. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

ИСПДн МЖКХиТЭК является информационной системой обработки персональных данных. Меры по обеспечению безопасности персональных данных и порядок их выбора, устанавливаются в соответствии с составом и содержанием мер, утвержденных приказом ФСТЭК России от 18.02.2013 г. № 21. Обработка персональных данных в ИСПДн МЖКХиТЭК осуществляется в соответствии с «Правилами обработки персональных данных в ИСПДн МЖКХиТЭК».

11. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА

12.1. Требования по обеспечению безопасности информации в ИСПДн МЖКХиТЭК на стадиях жизненного цикла

Безопасность информации, обрабатываемой системами и средствами обработки, хранения и передачи информации должна обеспечиваться на всех стадиях жизненного цикла ИСПДн МЖКХиТЭК с учетом всех сторон: разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений и организации.

На этапе создания и модернизации ИСПДн МЖКХиТЭК, разработка технических заданий, проектирование, создание и тестирование и приемка средств и систем защиты информации в ИСПДн МЖКХиТЭК осуществляется по согласованию с ответственным за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК с учетом действующих организационно-распорядительных документов и «Частной модель угроз и нарушителей безопасности персональных данных при их обработке в информационной системе персональных данных Министерства жилищно-коммунального хозяйства и топливно-энергетического комплекса Новгородской области».

В ходе выполнения проектных работ обоснование и принятие решения должно основываться на рекомендациях, представленных в ГОСТ 34.601-90 и ISO/IEC IS 15288-2002.

Ввод в действие, эксплуатация, снятие с эксплуатации применяемых систем и средств защиты информации должны осуществляться при непосредственном участии администратора безопасности и также с привлечением ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

В ходе проектирования должна обеспечиваться защита от угроз:

- неверной формулировки требований к системе или комплексу;
- выбора неадекватной модели системы (систем) защиты информации, в том числе неадекватного выбора процессов обеспечения безопасности информации и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в программное обеспечение ИСПДн МЖКХиТЭК;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований, предъявляемых к процессам обеспечения безопасности информации в ИСПДн МЖКХиТЭК;
- разработки некачественной документации;
- сборки систем или средств обработки, хранения и передачи информации разработчиком/производителем, приводящей к появлению недокументированных возможностей, либо к неадекватной реализации требований к защите информации;
- неверного конфигурирования средств защиты информации, включая средства защиты, встроенные в системное и прикладное программное обеспечение;
- приемки системы защиты информации, не отвечающей требованиям документов политики информационной безопасности;
- внесения недокументированных возможностей в ИСПДн МЖКХиТЭК в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов информационной безопасности.

Привлекаемые на договорной основе для выполнения работ по разработке и/или производству средств и систем защиты специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством Российской Федерации. При приобретении готовых средств обработки информации и/или комплексов автоматизации и связи, либо их компонентов, разработчиком должна быть предоставлена документация, содержащая описание защитных мер в отношении имеющихся угроз безопасности информации.

В договор (контракт) о поставке средств обработки информации и их компонентов включаются положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей документации на изделие, обеспечивающего возможность сопровождения данного средства (комплекса) и его компонентов без участия разработчика.

Требования к обеспечению безопасности информации в ИСПДн МЖКХиТЭК должны включаться во все договоры и контракты на проведение работ или оказание услуг на всех стадиях жизненного цикла ИСПДн МЖКХиТЭК. Ввод в эксплуатацию ИСПДн МЖКХиТЭК осуществляется на основании приказа Министерства после выполнения

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
полного комплекса организационных и технических мер защиты информации и проверки их эффективности.

Техническое обслуживание и ремонтные работы на оборудовании ИСПДн МЖКХиТЭК проводятся только уполномоченными сотрудниками Министерства (или в их присутствии).

Все процедуры, связанные с изменением конфигурации программных и программно-технических средств ИСПДн МЖКХиТЭК, проведением технического обслуживания и ремонтных работ на технических средствах, должны документироваться с указанием объемов и сроков выполненных работ, а также лиц (организаций) проводивших работы, в формулярах СВТ, применяемых в ИСПДн МЖКХиТЭК.

Правила закупки программных и программно-технических средств, включая средства защиты информации, представлены в Приложение 3.

12.2. Взаимодействие с внешними организациями

В процессах функционирования ИСПДн МЖКХиТЭК для выполнения работ по модернизации, сопровождению и технической поддержки, применяемых систем и средств обработки, хранения и передачи информации на основании заключенных с Министерством договоров могут привлекаться внешние организации.

Обмен служебной и иной конфиденциальной информацией, необходимой для выполнения внешней организацией взятых на себя обязательств, должен осуществляться в соответствии с заключенным между Министерством и внешней организацией Соглашением о конфиденциальности. Кроме этого, Соглашение о конфиденциальности должно определять (регламентировать) процедуры управления и контроля за выполнением внешней стороной взятых на себя обязательств по защите информации доступ к которой ей был предоставлен.

12.2.1. Идентификация рисков, связанных с привлечением внешней стороной

Соглашение о конфиденциальности должно предусматривать риски, связанные с привлечением внешней стороны к процессам функционирования ИСПДн МЖКХиТЭК.

При идентификации рисков необходимо учитывать следующие аспекты:

- удобство обработки информации внешней стороной;
- тип доступа внешней стороны к информации и к средствам её обработки, например:

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- физический доступ, например, в особые зоны ИСПДн МЖКХиТЭК закрытые для посторонних лиц, помещения, хранилища электронных документов;
 - логический доступ, например, к файлам, таблицам баз данных, к операционным системам СВТ ИСПДн МЖКХиТЭК;
 - удаленный доступ к внутренним сетевым ресурсам ИСПДн МЖКХиТЭК, и сетям, взаимодействующих с ИСПДн МЖКХиТЭК информационных систем;
- значение и важность информации, доступ к которой получает внешняя сторона;
 - необходимый контроль и меры защиты информационных, программных и других активов, не предназначенных для доступа внешней стороны;
 - персонал внешней стороны, включенный в процесс обработку информации, защита которой возложена на Министерство;
 - предоставляемую для организации доступа аутентификационную информацию;
 - различия в средствах и способах защиты информации, используемых в ИСПДн МЖКХиТЭК и в информационной системе внешней стороной;
 - организацию и технологии управления, совместно используемыми ресурсами;
 - возможность блокирования субъектов доступа внешней стороны к информации в случае нарушений требований к обеспечению безопасности в ИСПДн МЖКХиТЭК или внесения несогласованных изменений в процессы ее функционирования;
 - организацию взаимодействия и установленные процедуры разрешения инцидентов безопасности;
 - размеры ущерба (потенциальные убытки), в случае нарушений внешней стороной правил и требований к обеспечению безопасности информации;
 - требования нормативов, стандартов и законов РФ, другие договорные обязательства, уместные в рамках взаимоотношений с внешней стороны, которые необходимо принимать во внимание;
 - интересы любых других заинтересованных сторон, которые могут быть затронуты в случае предоставления конфиденциальной информации внешней стороне.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
12.2.2. Защита информационных ресурсов при работе с внешней стороной

Соглашения с вовлечением внешней стороны, использующей: доступ, обработку, коммуникации, управление ресурсами ИСПДн МЖКХиТЭК должны учитывать требования к обеспечению безопасности персональных данных и иной обрабатываемой в ИСПДн МЖКХиТЭК информации, в части предоставления защищенного доступа к информационным ресурсам ИСПДн МЖКХиТЭК.

При определении ответственности внешней стороны, допущенной к работе с ИСПДн МЖКХиТЭК, необходимо учитывать:

- наличие и выполнение совместно принятых решений, правил, регламентов и процедур обеспечения безопасности информации;
- использование внешней стороной организационных и организационно-технических мер защиты информации, включая обеспечение контроля (мониторинга) защищенности, взаимодействующих с ИСПДн МЖКХиТЭК СВТ.
- наличие подготовленного для выполнения работ персонала, обученного методам безопасной работы с ресурсами ИСПДн МЖКХиТЭК;
- наличие установленных форм отчетности и правил согласования форматов сообщений передаваемой информации;
- наличие политики контроля доступом, охватывающей и учитывающей:
 - требования о необходимости доступа внешней стороны к ресурсам ИСПДн МЖКХиТЭК;
 - разрешенные методы доступа и управления ресурсам ИСПДн МЖКХиТЭК;
 - регламентацию процесса предоставления доступа и предоставляемые привилегии, включая правила отмены прав доступа субъектов и/или прекращения дальнейшего использования ими предоставленного доступа;
 - требования по поддержанию списка лиц, уполномоченных использовать доступные службы и сервисы, их права и обязанности;
- использование, принятых в рамках Соглашений о конфиденциальности, процедур передачи сообщений, уведомлений, а также процедур проведения расследований инцидентов безопасности и/или нарушений требований к обеспечению безопасности информации;
- возможности по обеспечению прав проведения контроля и отмены действия, связанных с доступом к ресурсам ИСПДн МЖКХиТЭК внешней стороной;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- определение обязанностей сторон по организации аудита безопасности, а также аудита безопасности третьей стороны (при необходимости), с указанием предоставленных аудиторам прав;
- регламентации в Соглашении о конфиденциальности действий сторон в случае возникновения нештатных ситуаций;
- требования к обеспечению непрерывности технологических процессов ИСПДн МЖКХиТЭК, включая меры по обеспечению доступности и доступности, в соответствии с установленными приоритетами технологических процессов ИСПДн МЖКХиТЭК;
- наличие взаимных обязательств, относительно решения юридических вопросов и обеспечения требований законодательных актов, например, законодательства по защите персональных данных;
- юридический контроль принятых на себя внешней стороной обязательств;
- обеспечение внешней стороной защиты персональных данных, интеллектуальной собственности, авторского права и иных сведений, подлежащих защите;
- возможность осуществления контроля с привлечения третьей стороны;
- обеспечение условий для пересмотра/отмены соглашений о конфиденциальности.

При необходимости требования к процедурам, регламентирующим защиту ресурсов ИСПДн МЖКХиТЭК при взаимодействии с внешней стороной, могут быть расширены.

Если управление безопасностью информации в ИСПДн МЖКХиТЭК предполагает аутсорсинг внешней стороны, Соглашение о конфиденциальности должно гарантировать достаточный уровень обеспечения безопасности информации и возможность выполнения взятых на себя обязательств при изменении существующих информационных рисков.

12.2.3. Соглашения о конфиденциальности

В Соглашении о конфиденциальности должны быть предусмотрены процедуры, учитывающие условия для продолжения информационного обмена, в случаях, когда внешняя сторона становится неспособной обеспечить поддержку взятых на себя обязательств.

Соглашение о конфиденциальности должно учитывать интересы других заинтересованных сторон, условия их участия и требования, заключенных с ними соглашений.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Условия соблюдения режима безопасности (в частности, неразглашение, ставших известными, защищаемых в ИСПДн МЖКХиТЭК персональных данных и иных конфиденциальных сведений) должны содержать требования к защите конфиденциальности и иные требования к защите информации, составленные в юридически согласованных терминах и обеспечивающих недопущение фактов нанесения материального, морального или иного ущерба субъектам персональных данных и Министерству, как оператору персональных данных.

Соглашение о конфиденциальности должно включать в себя:

1. Определение и уровень критичности информации, подлежащей защите;
2. Срок действия соглашения о конфиденциальности, включая случаи, где конфиденциальность может быть сохранена неограниченное время;
3. Необходимые действия по истечению срока соглашения;
4. Права и обязанности сторон, подписавших соглашение о конфиденциальности (неразглашения) сведений, ставших известными, либо переданными, в рамках совместной деятельности сторон, в том числе и в одностороннем порядке. Формулировки соглашения, определяющие обязанности по соблюдению конфиденциальности, должны содержать записи типа - «необходимо знать», «необходимо выполнять»;
5. Порядок монопольного использования информации: коммерческих секретов, интеллектуальной собственности и т.д., полученных от противоположенной стороны подписного соглашения;
6. Разрешенное использование конфиденциальной информации и прав доступа к ней сотрудниками сторон, подписавших соглашение;
7. Права на ревизию и проведение мероприятий контроля действий противоположенной стороны, по использованию переданной (полученной) ею информации и/или прав доступа противоположной стороны по ее использованию;
8. Порядок уведомления противоположной стороны о несанкционированном раскрытии переданной информации или нарушении ей, принятого в рамках соглашения, режима конфиденциальности;
9. Условия, определяющие порядок возврата или уничтожения полученной от противоположенной стороны информации, после завершения или прекращения действия принятого соглашения;
10. Санкции (действия), которые будут предприняты в случае нарушения принятого соглашения.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Соглашение о конфиденциальности (о неразглашении) должно учитывать все принятые в РФ законы и правила для юрисдикции, а также требования организационно-распорядительные документов Министерства, в рамках которой они применяются.

Требования о конфиденциальности (соглашения о неразглашении) должны периодически, либо внепланово пересматриваться, с учетом изменений в технологиях информационного взаимодействия сторон, а также при возникновении других обстоятельств и условий, при которых прежние требования не отвечают интересам сторон.

Контроль за выполнением требований Соглашения о конфиденциальности должен охватывать:

- поставщиков услуг;
- задействованные административно-технические подразделения внешней стороны;
- управление процессам деятельности представителей внешней стороны;
- компании-разработчиков и поставщиков, например, программных изделий и IT-систем;
- обслуживающие организации, например, обеспечивающие охрану, обслуживание систем жизнеобеспечения, уборку помещений, доставку продукции и другие поддерживающие аутсорсинговые службы;
- временный персонал и иные краткосрочные назначения.

Пример договора «О соблюдении конфиденциальности персональных данных» представлен в Приложении 5 настоящего Положения.

12.3. Планирование и приемка компонентов подсистем защиты информации

Целью планирования и приемки компонентов систем и средств защиты информации в ИСПДн МЖКХиТЭК является снижение рисков, связанных с неисправностями используемых средств защиты информации.

В рамках эксплуатации систем и средств защиты информации должны обеспечиваться долгосрочное планирование и подготовка ИСПДн МЖКХиТЭК к развертыванию новых компонентов системы защиты персональных данных. Подготовка должна гарантировать доступность, адекватную и готовность ресурсов ИСПДн МЖКХиТЭК к интеграции (модификации) в рамках новых проектных решений компонентов подсистем защиты без снижения ранее достигнутого уровня безопасности.

12.3.1. Принятие систем (компонентов системы) защиты информации

Принятие систем (компонентов системы) защиты информации в эксплуатацию должно основываться на решении руководства Министерства, представленном в виде приказа о вводе системы (компонента) системы защиты в эксплуатацию. В ряде случаев принятие систем (компонентов системы) защиты информации может быть совмещено с принятием в эксплуатацию систем (подсистем) ИСПДн МЖКХиТЭК, предназначенных для обеспечения автоматизации основных производственных процессов. В этом случае в решении руководства должно быть явно указано целевое назначение систем (компонентов) системы защиты, а также категории должностных лиц, ответственных за ее эксплуатацию.

Руководство Министерства должно гарантировать, что требования для принятия новых систем (компонентов системы) защиты информации ясно определены, согласованы, задокументированы и испытаны. Новые средства защиты, их обновления и новые версии в случае применения программных средств защиты, должны быть перемещены в среду эксплуатации только после получения формального разрешения в виде приказа о вводе в эксплуатацию.

Для получения официального разрешения на ввод в эксплуатацию должны быть выполнены следующие требования:

- в ходе проведения тестовых испытаний получены эксплуатационные характеристики системы и/или средства защиты, проведен анализ соответствия их требованиям документов политики информационной безопасности, а также требования к производительности, надежности и качества;
- определены, протестированы и приняты к исполнению процедуры восстановления работоспособности, процедуры рестарта и регламенты действий во внештатных ситуациях;
- определен, протестирован и принят к исполнению согласованный набор мер защиты, управления и мониторинга состояния;
- определены эффективные процедуры управления;
- приняты меры по обеспечению непрерывности процесса функционирования;
- имеются результаты (объективные доказательства) того, что новая система (компонент системы) защиты не будет неблагоприятно воздействовать на существующие компоненты, особенно в пиковые интервалы нагрузки;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- доказательство того, что новая система (компонент системы) защиты не повлияет отрицательно на производительность, используемых ИСПДн МЖКХиТЭК СВТ;
- обслуживающий персонал и иные полномочные субъекты доступа прошли обучение;
- проведена оценка эффективности системы (компонентов системы) защиты, на предмет минимизации возможных ошибок и иных деструктивных воздействий со стороны пользователей и обслуживающего ИСПДн МЖКХиТЭК персонала.

12.3.2. Процесс подключения новых средств защиты информации

Процесс подключения новых средств защиты информации должен учитывать требования:

1. Подключение новых средств защиты должны быть согласовано с ответственными за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.
2. Одобрение следует также получать от должностных лиц, ответственных за обеспечение физической защиты оборудования ИСПДн МЖКХиТЭК (например, руководства подразделения охраны). Это обеспечивает уверенность в том, что все соответствующие требования к обеспечению безопасности среды функционирования ИСПДн МЖКХиТЭК выполняются.
3. Все вводимые в эксплуатацию программные и программно-технические средства защиты, где необходимо, должны быть проверены на совместимость с компонентами взаимодействующих систем и средства, используемых в ИСПДн МЖКХиТЭК.

12.4. Безопасность разработки и сопровождения программного обеспечения

Целью обеспечения безопасной разработки и сопровождения программного обеспечения является защита программного обеспечения от угроз несанкционированной модификации и/или не умышленного искажения на этапах разработки и сопровождения.

Выполняемые, в рамках различных проектов работы по созданию программного обеспечения, а также средства их поддержки и инструментарий разработки должны строго управляться и контролироваться.

Примечание - *Ответственность за выполнение требований по защите программного обеспечения в ходе разработки и сопровождении программного обеспечения наряду с непосредственными исполнителями должны нести и*

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
администраторы (персонал), в обязанности которых входит обеспечение и поддержка среды разработки и сопровождения программного обеспечения в соответствии с принятым регламентом.

Они должны гарантировать, что все предложенные изменения по созданию среды разработки и сопровождения рассмотрены, созданы и проверены на соответствие требованиям документов политики информационной безопасности.

12.4.1. Управление изменениями конфигураций средств защиты информации

Основной целью управления изменениями конфигураций средств защиты информации в процессах обеспечения безопасности информации в ИСПДн МЖКХиТЭК является повышение их эффективности.

Внесение изменений в конфигурации средств защиты информации необходимо выполнять в соответствии с проектной документацией, техническими требованиями производителей, нормативными актами полномочных органов государственной власти и государственным стандартами Российской Федерации в области защиты информации.

Процесс внесения изменений в конфигурации средств защиты информации должен включать в себя оценку информационных рисков, анализ изменений в основных процессах функционирования ИСПДн МЖКХиТЭК, также оценку соответствия требований документов политики информационной безопасности ИСПДн МЖКХиТЭК.

Процесс внесения изменений в конфигурации средства защиты информации должен также гарантировать, что данное средство защиты не будет скомпрометировано.

Процедуры управления изменения в конфигурациях средств защиты информации должны включить в себя:

- согласование изменений в соответствии с принятым решением, определяющим и устанавливающим необходимость их внесения;
- оценку существующих механизмов управления и процедур контроля целостности, результаты которой гарантируют то, что выполненные изменения не приведут к компрометации системы защиты и ИСПДн МЖКХиТЭК в целом;
- выполнение (проведение) изменений только уполномоченным персоналом ИСПДн МЖКХиТЭК;
- идентификацию и инвентаризацию всего программного обеспечения, информации, объектов баз данных и программных и программно-технических средств, которые подвергаются изменениям, в том числе и условий среды их функционирования;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- получение официального одобрения на проведение изменений перед началом работы;
- контроль того, что комплект технической документации был модифицирован с учетом каждого изменения, а старая документация заархивирована или уничтожена в установленном порядке;
- контроль соответствия используемых версий программного обеспечения с версиями, принятыми к использованию;
- поддержание и сохранение результатов аудита всех контролируемых систем и средств обработки, хранения и передачи информации;
- контроль того, что вся технологическая (рабочая) документация и руководства (инструкции) поддерживаются в актуальном состоянии;
- проведение мониторинга состояния СВТ ИСПДн МЖКХиТЭК.

Изменения, связанные с обновлениями программного обеспечения, подлежат обязательному тестированию в среде, эмулирующей среду функционирования ИСПДн МЖКХиТЭК.

Механизмы автоматического обновления программного обеспечения с функциями обеспечения безопасности информации не должны использоваться на критичных для функционирования ИСПДн МЖКХиТЭК СВТ.

12.4.2. Технологическая проверка прикладного программного обеспечения после изменений (обновлений) операционной системы

При проведении изменений (обновлений) операционных систем СВТ используемое в их среде прикладное программное обеспечение, а также программное обеспечение СУБД, должно быть протестировано до проведения изменений в ИСПДн МЖКХиТЭК.

Выполнение данного требования гарантирует отсутствие неблагоприятных воздействий на процессы функционирования ИСПДн МЖКХиТЭК прикладного уровня и используемые в них механизмы защиты информации.

Требования к технологической проверке (тестированию) должны включать в себя:

- пересмотр механизмов и приемов управления прикладными процессами и процедурами контроля их целостности, чтобы гарантировать, что они не были скомпрометированы изменениями операционной системы;
- обеспечение уверенности в том, что меры по поддержке непрерывности технологических процессов ИСПДн МЖКХиТЭК покрывают издержки на пересмотр технической политики (процедур, регламентов, методов, механизмов и процессов) и обеспечивает тестирование прикладных систем

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
(приложений) после проведения соответствующих изменений в операционных системах СВТ;

- обеспечение того, чтобы сообщения об изменениях (обновлениях) операционных систем поступали своевременно и из доверенного источника;
- поддержку в актуальном состоянии технологической (рабочей) документации, принятых мер обеспечения непрерывности процессов функционирования ИСПДн МЖКХиТЭК, при проведении процедур, связанных с изменениями в системном программном обеспечении.

Ответственность за выполнение требований по организации и проведению изменений в программное обеспечение ИСПДн МЖКХиТЭК возлагается на ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК, в обязанности которых входит контроль, имеющих место уязвимостей при получении и установки новых исправлений (обновлений) программного обеспечения.

12.4.3. Ограничения на изменения пакетов используемого программного обеспечения

Проведения изменений используемых программ, входящих в состав пакетов программного обеспечения, установленного на СВТ ИСПДн МЖКХиТЭК, могут быть запрещены или ограничены в использовании.

Пакеты программ, полученные непосредственно от производителей/вендоров¹³, после проверки их целостности могут использоваться без внесения изменений.

В том случае, когда пакет применяемых в ИСПДн МЖКХиТЭК программ должен измениться, выполняются следующие требования:

- проводится оценка потенциальных рисков с целью выявления возможной компрометации процессов функционирования ИСПДн МЖКХиТЭК;
- получено согласие от поставщика на проведение изменений;
- поставщик гарантирует возможность возврата (отката) программного обеспечения к предыдущей версии.

Если изменения необходимы, первоначальное программное обеспечение должно быть сохранено, а изменения должны быть внесены в идентифицированную копию пакета.

В случае необходимости, изменения должны быть проверены и подтверждены независимой оценочной комиссией.

¹³ Разработчики программного обеспечения

12.4.4. Вопросы утечки информации в ходе разработки и сопровождения программного обеспечения

Для минимизации риска утечки информации в ходе разработки и сопровождения программного обеспечения должны быть приняты меры закрытия потенциальных каналов утечки информации.

Принятые меры должны минимизировать риск утечки информации, например, при использовании и эксплуатации каналов связи, выходящих за границу сетевого периметра ЛВС ИСПДн МЖКХиТЭК.

Для этого в ИСПДн МЖКХиТЭК должны применяться следующие меры защиты:

- обеспечиваться контроль выносимых за границу контролируемой зоны съемных носителей информации; При этом должна выполняться проверка отсутствия на носителях информации с защищаемыми сведениями, с учетом наличия остаточной информации и приемов ее сокрытия;
- при передаче информации по каналам связи, выходящим за границу сетевого периметра, должны использоваться средства криптографической защиты, снижающие вероятность перехвата информации злоумышленником;
- для организации каналов удаленного доступа к СВТ ИСПДн МЖКХиТЭК должны применяться сертифицированные средства криптографической защиты сетевого трафика;
- должен проводиться регулярный аудит и контроль действий субъектов доступа в соответствии с требованиями к обеспечению безопасности информации;
- соблюдаться установленный порядок управления (регламентации) информационными ресурсами ИСПДн МЖКХиТЭК.

12.4.5. Вопросы защиты информации при разработке программного обеспечения внешней стороной

Программное обеспечение, которое разрабатывается внешней стороной должно контролироваться и проверяться администратором безопасности ИСПДн МЖКХиТЭК.

Если программное обеспечение приобретено у внешнего разработчика, то ответственный за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК обязан получить свидетельства, подтверждающие наличие:

- лицензионного соглашения, права на монопольное использование программного кода и права на интеллектуальную собственность;
- сертификата качества и соответствие его требованиям Российского законодательства;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- соглашения о разрешении споров в случае претензий от внешней, либо к внешней стороне;
- права Министерства на проведение аудита качества, разрабатываемого программного обеспечения;
- гарантий на проведение испытания перед инсталляцией на предмет обнаружения вредоносного кода.

12. ТРЕБОВАНИЯ К ОРГАНИЗАЦИЯМ, ПРЕДОСТАВЛЯЮЩИМ УСЛУГИ ПО СОПРОВОЖДЕНИЮ, ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ, МОДЕРНИЗАЦИИ И ВНЕДРЕНИЮ НОВЫХ СИСТЕМ И СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ, ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ

Для проведения работ по сопровождению, технической поддержке, модернизации и внедрению новых систем и средств обработки, хранения, передачи и защиты информации Министерством могут привлекать проектные и обслуживающие организации (подрядчики) с которыми установлены договорные отношения.

Для выполнения ими взятых на себя обязательств обслуживающему персоналу таких организаций может потребоваться временное предоставление удаленного доступа к СВТ ИСПДн МЖКХиТЭК.

Условиями предоставления удаленного доступа персоналу проектных и обслуживающих организаций являются:

1. Услуги, предоставляемые организацией должны быть юридически оформлены в форме заключенных между Министерством и внешней организацией договора(ов) на предоставление услуг (выполнение работ);
2. Удаленного доступа персонала внешней организации может предоставляться только временно, на период необходимый для выполнения работ в соответствии с договорными обязательствами, взятыми на себя подрядной организацией. Постоянный доступ к СВТ ИСПДн МЖКХиТЭК запрещен.
3. Должностные лица из числа персонала подрядной организации должны быть допущены к выполнению работ на оборудовании ИСПДн МЖКХиТЭК на основании приказа руководителя.
- 4.
5. Все работы персонала внешней организации должны контролироваться сотрудником Министерства, назначенным от лица Министерства осуществлять контроль и сопровождение работ, выполняемых подрядной организацией.

В процессах функционирования ИСПДн МЖКХиТЭК может взаимодействовать с внешними информационными системы персоналу которых предоставляется удаленный доступа к ресурсам ИСПДн МЖКХиТЭК.

В качестве СВТ подрядной организации с которых может быть разрешен удаленный доступ к СВТ ИСПДн МЖКХиТЭК должны рассматриваться АРМ

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
администраторов и иных лиц из числа технического персонала, являющихся работниками внешней организации с правом выполнения работ на оборудовании ИСПДн МЖКХиТЭК.

13.1. Требования к размещению СВТ с которых разрешен удаленного доступа из информационных систем подрядных организаций

Доступ в помещения, в которых размещены СВТ с которых разрешен удаленного доступа из внешних информационных систем подрядных организаций, должен запрещен посторонним лицам по роду своей деятельности не допущенным к проведению работ в ИСПДн МЖКХиТЭК.

13.2. Требования к хранению бумажных и машинных носителей с конфиденциальной информацией, переданной Министерством подрядной организации

Бумажные документы и машинные носители с конфиденциальной информацией, переданные подрядной организации для выполнения работ в соответствии с договорными обязательствами, должны храниться в запираемом шкафу или сейфе, опечатанном печатью ответственного должностного лица подрядной организации назначенного приказом руководителя.

13.3. Требования к программно-аппаратной среде СВТ с которых разрешен удаленного доступа из информационных систем подрядных организаций

Для выполнения работ по установке и администрированию системного, прикладного и специального программного обеспечения на СВТ с которых разрешен удаленного доступа из информационных систем подрядных организаций к СВТ ИСПДн МЖКХиТЭК допускаются только лица из числа административно-технического персонала подрядной организации, наделенные соответствующими полномочиями в соответствии с требованиями и правилами, представленными в разделе 5 настоящего Положения.

К процессам эксплуатации СВТ с которых разрешен удаленного доступа из информационных систем подрядных организаций к СВТ ИСПДн МЖКХиТЭК предъявляются следующие требования:

- должно использоваться только лицензионное программное обеспечение;
- установка программного обеспечения должна осуществляться только с оригинальных носителей, входящих в комплект поставки, либо с их копий;
- установка и использование программных средств, непредназначенных для выполнения работ в соответствии с обязательствами подрядной организацией перед Министерством запрещены;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- конфигурации, применяемого системного, прикладного и специального программного обеспечения должны исключать возможность удаленного доступа (подключения) к СВТ с которых разрешен удаленного доступа к СВТ ИСПДн МЖКХиТЭК;
- СВТ с которых разрешен удаленного доступа к СВТ ИСПДн МЖКХиТЭК не должны находиться под управлением систем централизованного управления типа Active Directory;
- запрещается установка и использование средства разработки и отладки программного обеспечения;
- руководством подрядной организацией должны быть приняты меры, исключающие возможность несанкционированного изменения состава и конфигурацией аппаратной части СВТ с которых разрешен удаленного доступа к СВТ ИСПДн МЖКХиТЭК (например, путем опечатывания системных блоков печатью администратора безопасности подрядной организации).

13.4. Требования к средствам защиты АРМ подрядной организации, с которых разрешен удаленного доступа к СВТ ИСПДн МЖКХиТЭК

Для защиты АРМ подрядной организации, с которых разрешен удаленного доступа к СВТ ИСПДн МЖКХиТЭК, должны применяться:

- средства криптографической защиты не ниже класса КСЗ;
- средства вычислительной техники не ниже 5 класса защищенности от несанкционированного доступа;
- средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса.

13. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Целью управления инцидентами безопасности и механизмами ответной реакции на их проявление является обеспечение выбора и реализация непротиворечивого и эффективного способа локализации и устранения возникающих в ИСПДн МЖКХиТЭК инцидентов безопасности информации.

При возникновении инцидента безопасности сотрудник, обнаруживший его проявление, обязан немедленно поставить в известность администратора безопасности и своего непосредственного руководителя.

Администратор безопасности проводит анализ сложившейся ситуации на предмет констатации инцидента безопасности, принимает меры по его разрешению и уведомляет ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК о факте инцидента и принятых мерах.

Особое внимание администратор безопасности должен уделять контроль за состоянием процессов сбора и регистрации (записи, хранения, передачи) событий безопасности. Сбои и иные нарушения в работе систем и средств обеспечения сбора и регистрации должны рассматриваться как критичные для функционирования ИСПДн МЖКХиТЭК инциденты безопасности информации.

В случае возникновения сбоя в процессах сбора и регистрации событий безопасности администратор безопасности или иное полномочное должностное лицо, ответственное за сбор и регистрацию событий безопасности, обязано принять меры по локализации и устранению возникшей проблемы путем:

- снижения частоты сбора событий безопасности;
- отключения мониторинга части объектов контроля;
- удаления устаревших данных (событий безопасности);
- принятия иных мер, обеспечивающих работоспособность систем и средств обеспечения сбора и регистрации (записи, хранения, передачи) событий безопасности.

По окончании мероприятий по разрешению выявленного инцидента безопасности администратором безопасности составляется акт с описанием сложившейся ситуации. К акту прилагаются (при наличии) поясняющие материалы (копии экрана, распечатка журнала событий и др.).

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

При необходимости в Министерстве назначается комиссия и проводится служебное расследование по факту возникновения нештатной ситуации и выяснению причин ее возникновения.

Типовые действия персонала ИСПДн МЖКХиТЭК при инцидентах безопасности информации представлены в Приложении 4 Положения.

14. ОБУЧЕНИЕ И ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ ПЕРСОНАЛА ИСПДн МЖКХиТЭК

15.1. Общие положения

Все сотрудники Министерства, а также представители (административно-технического персонал) от внешних организаций, являющиеся авторизованными пользователями ИСПДн МЖКХиТЭК или задействованные в процессах ее обслуживании, должны пройти соответствующее обучение, целью которого является понимание и осознание необходимости обеспечения безопасности информации в ИСПДн МЖКХиТЭК.

В инструктажи и тренинги для персонала ИСПДн МЖКХиТЭК включается: изучение требований по защите информации, обязанности, порядок и правил использования средств контроля состояния защищенности информации, а также процедуры безопасного использования средств обработки информации.

Форма журнала инструктажа по мерам обеспечения безопасности информации в ИСПДн МЖКХиТЭК и выполнению правил работы со средствами защиты информации представлена в Приложении 2.

Ответственность за организацию своевременного и качественного обучения и повышения осведомленности персонала ИСПДн МЖКХиТЭК, а также за проведение проверки полученных знаний, возлагается на администратора безопасности, а в подразделениях обслуживания на руководителей данных подразделения.

Контроль выполнения плановых мероприятий (занятий) по повышению осведомленности и обучению персонала ИСПДн МЖКХиТЭК по вопросам защиты информации в ИСПДн МЖКХиТЭК осуществляет руководители подразделений.

15.2. Вводный инструктаж

Вводный инструктаж проводится с каждым сотрудником Министерства, включая принимаемых на работу или переводимых на новое место работы руководителей подразделений; с представителями сторонних организаций, в случае предоставления им доступа к защищаемым информационным ресурсам ИСПДн МЖКХиТЭК; с другими лицами, которые участвуют в процессах обеспечения работоспособности ИСПДн МЖКХиТЭК.

15.3. Первичный инструктаж

Первичный инструктаж с сотрудниками Министерства проводит непосредственный руководитель, который в свою очередь прошёл обучение (инструктаж) у администратора безопасности ИСПДн МЖКХиТЭК и успешно сдал зачет по знанию требований к обеспечению безопасности информации в части его касающейся.

Первичный инструктаж проводится:

- со всеми принятыми на работу работниками;
- с работниками, переведенными из другого структурного подразделения;
- с работниками, которым поручено выполнение новой для них работы;
- с командированными работниками сторонних организаций;
- с другими лицами, участвующие в процессах функционирования ИСПДн МЖКХиТЭК.

От первичного инструктажа освобождаются работники, работа которых не связана с использованием, обслуживанием, эксплуатацией, испытанием, ремонтом и наладкой оборудования ИСПДн МЖКХиТЭК.

Факт проведения первичного инструктажа по мерам обеспечения безопасности информации подтверждается собственноручной подписью проинструктированного лица, с указанием даты его проведения.

15.4. Внеплановый инструктаж

Внеплановый инструктаж по мерам обеспечения безопасности информации в ИСПДн МЖКХиТЭК проводится в следующих случаях:

- при внесении изменений или введении в действие новых нормативных и правовых актов Российской Федерации, внутренних организационно-распорядительных документов, регламентирующих требования к организации защиты информации ИСПДн МЖКХиТЭК или изменении состава ранее принятых к исполнению обязанностей;
- при вводе в эксплуатацию, модернизации или замены оборудования и/или программного обеспечения ИСПДн МЖКХиТЭК;
- при изменениях в процессах обработки защищаемая информация;
- по требованию должностных лиц органов государственного контроля и надзора;
- при нарушении субъектом доступа требований к обеспечению безопасности информации;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

– при перерыве в работе (более чем на 60 календарных дней).

15.5. Формы проведения занятий

Занятия по вопросам обеспечения безопасности информации в ИСПДн МЖКХиТЭК проводятся в форме: лекций, семинаров, практических и индивидуальных занятий, консультаций, самоподготовки, тренинга с использованием различных видов тренажеров, включая компьютерные курсы.

Приложение 1

Форма заявки

ЗАЯВКА
НА ВНЕСЕНИЕ ИЗМЕНЕНИЙ В СПИСКИ ПОЛЬЗОВАТЕЛЕЙ ИСПДн МЖКХиТЭК
И НАДЕЛЕНИЯ ПОЛНОМОЧИЯМИ ДОСТУПА К РЕСУРСАМ СИСТЕМЫ

Прошу зарегистрировать (изменить полномочия) в ИСПДн МЖКХиТЭК и предоставить доступ к

(перечислить оборудование, информационные сервисы, сетевые ресурсы)

(должность с указанием подразделения, организации)

(фамилия имя и отчество сотрудника)

и предоставив полномочия, необходимые для работы с информационными ресурсами:

(список информационных ресурсов с указанием в скобках прав: чтение, запись, изменение, выполнение)

Предыдущие полномочия данного пользователя отменить (не отменять).

(ненужное зачеркнуть)

Должность

(наименование заказывающего подразделения, организации)

«__» _____ 201__ г.

(подпись)

(фамилия)

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Приложение 2
Формы журналов

ФОРМЫ ЖУРНАЛЫ

ЖУРНАЛ

учета съемных машинных носителей информации

Начат _____

Окончен _____

| № п/п | Дата, учетный номер | Серийный номер (заводской номер) | Тип и модель | Место хранения | Кому передан | Получено (подпись, дата) | Возвращено (подпись, дата) | Отметка об уничтожении (№ и дата акта) |
|-------|---------------------|----------------------------------|--------------|----------------|--------------|--------------------------|----------------------------|--|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | | |

ЖУРНАЛ

учета мест хранения съемных машинных носителей информации

Начат _____

Окончен _____

| № п/п | Инвентарный номер | Расположение (этаж, кабинет) | Ответственный за хранилище | Дата установки | Дата и № акта списания | Подпись ответственного лица |
|-------|-------------------|------------------------------|----------------------------|----------------|------------------------|-----------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |

ЖУРНАЛ

технического обслуживания

(наименование оборудования)

| № п/п | Дата проведения мероприятия | Основание для проведения мероприятия | Проведенные работы | Ф.И.О. ответственного | Расписка о проведении мероприятия |
|-------|-----------------------------|--------------------------------------|--------------------|-----------------------|-----------------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 |

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

| | | | | | |
|--|--|--|--|--|--|
| | | | | | |
|--|--|--|--|--|--|

ЖУРНАЛ

контроля выполнения требований, предъявляемых к обеспечению безопасности информации в
ИСПДн МЖКХиТЭК

| № п/п | Дата проведения мероприятия | Основание для проведения мероприятия | Проведенные работы | Ф.И.О. ответственного | Расписка о проведении мероприятия |
|----------|--------------------------------|--|-----------------------|--------------------------|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |

ЖУРНАЛ

инструктажа по мерам обеспечения безопасности информации в ИСПДн МЖКХиТЭК и
выполнению правил работы со средствами защиты информации

| № п/п | Дата | Ф.И.О. и должность инструктируемого | Подразделение | Тема инструктажа | Подпись | Инструктаж провел |
|----------|------|--|---------------|---------------------|---------|----------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |

Примечание - Журнал заполняется администратором безопасности, либо лицом, исполняющим его обязанности. Регистрации в журнале подлежат сотрудники из числа персонала ИСПДн МЖКХиТЭК, прошедшие инструктаж и получившие допуск к работе в ИСПДн МЖКХиТЭК.

В графе 1 указываются порядковые номера инструктируемых сотрудников.

В графе 2 указывается дата проведения инструктажа.

В графе 3 и 4 указывается ФИО, должность сотрудника и подразделение в котором он работает соответственно.

В графе 5 указывается краткое содержание, либо тема инструктажа.

В графе 6 сотрудник расписывается по факту проведения инструктажа.

В графе 7 администратор безопасности расписывается в факте проведения инструктажа, если инструктаж проводил сотрудник временно исполняющий обязанности администратора безопасности, то вносятся ФИО и должность сотрудника.

ПРАВИЛА ЗАКУПКИ ПРОГРАММНЫХ И ПРОГРАММНО- ТЕХНИЧЕСКИХ СРЕДСТВ

1. Общие положения

Настоящие правила устанавливают требования к организации работ по приобретению для нужд Министерства жилищно-коммунального хозяйства и топливно-энергетического комплекса (далее Министерство) программного обеспечения, средств обработки информации и средств защиты информации, в части вопросов, касающихся требований к обеспечению безопасности информации.

Правила регламентируют действия сотрудников Министерства при выполнении работ по закупке программных и программно-технических средств обработки, хранения, передачи и защиты информации.

2. Порядок приобретения программного обеспечения

При выборе общесистемного, специального и прикладного программного обеспечения преимущество отдается продукту (продуктам), имеющему подтверждение независимых экспертов (декларация, сертификат) о наличии необходимых встроенных функций безопасности информации.

При приобретении общесистемного программного обеспечения лицо, ответственное за его приобретение, должно обеспечить наличие лицензий на использование приобретаемого программного обеспечения.

При необходимости разработки специального и прикладного обеспечения осуществляется его заказ в организации-разработчике. Выбор организации-разработчика должен осуществляться на конкурсной основе в соответствии с установленным в Министерстве порядком.

Разработка специального и прикладного обеспечения должна осуществляться на основании Технического задания, которое должно содержать специальный раздел, посвященный вопросам защиты информации. Специальный раздел Технического задания разрабатывается заказывающим подразделением и согласуется с ответственным за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

С полученного от организации-разработчика дистрибутива программного обеспечения системный администратор, ответственный за его использование, изготавливается рабочие копии, которые в дальнейшем используются для его установки (инсталляции).

Исключения могут составлять носители информации, с которых невозможно изготовить копии по причине защиты от копирования или по требованиям организации-разработчика.

Все дистрибутивы (оригиналы полученного от организации-разработчика программного обеспечения) должны маркироваться и регистрироваться в специальном журнале учета программного обеспечения, используемого в ИСПДн МЖКХиТЭК.

Системные администраторы, ответственные за установку и настройку полученного от организации-разработчика программного обеспечения производят его установку и настройку только с рабочих копий.

До начала работ по установке программного обеспечения системный администратор осуществляет антивирусную проверку программного обеспечения (ПО), устанавливаемого в пределах своих полномочий и получаемого от разработчика (поставщика, дистрибьютора).

По завершению работ по установке (инсталляции) полученного от организации-разработчика программного обеспечения носители информации с дистрибутивы программного обеспечения передаются администратору безопасности для хранения в библиотеке дистрибутивов программного обеспечения ИСПДн МЖКХиТЭК.

3. Порядок приобретения средств обработки информации

Приобретение средств обработки информации осуществляется на основании решения о модернизации ИСПДн МЖКХиТЭК. При выборе средств обработки информации предпочтение отдается оборудованию тех организаций-разработчиков, которые имеют подтверждение независимых экспертов (декларация, сертификат) о наличии необходимых встроенных функций безопасности информации.

Состав и спецификация закупаемого оборудования согласуется с ответственным за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

При необходимости могут организовываться дополнительные проверки средств обработки информации (тестирование или сертификационные испытания).

4. Порядок приобретения средств защиты информации

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-
ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Специальные (сертифицированные) средства защиты информации выбираются из числа имеющихся в настоящее время на рынке.

При выборе специальных (сертифицированных) средств защиты информации предпочтение отдается тем средствам защиты информации, которые имеют подтверждение в виде сертификата соответствия требованиям полномочного органа исполнительной власти Российской Федерации в области защиты информации.

Приобретаемые средства защиты информации по возможности должны функционировать на единой стандартизированной технологической основе и в максимальной степени учитывать требования установленного комплекса организационных, инженерно-технических и технических мер, обеспечивающих функционирования ИСПДн МЖКХиТЭК.

При выборе средств защиты информации должны учитываться их возможности по сохранению своих защитных функций при изменениях в конфигурациях программных и программно-технических средств, применяемых в ИСПДн МЖКХиТЭК.

Выбираемые средства защиты информации не должны снижать установленный уровень защищенности ресурсов ИСПДн МЖКХиТЭК.

ТИПОВЫЕ ДЕЙСТВИЯ ПРИ ИНЦИДЕНТАХ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. Действия при стихийных бедствиях, пожарах или наводнениях

При возникновении нештатной ситуации, работник обязан:

- оповестить других работников;
- оповестить соответствующие службы (пожарная охрана, служба спасения);
- сообщить непосредственному руководителю и администратору безопасности;
- принять меры к эвакуации оборудования ИСПДн МЖКХиТЭК и устранения последствий стихийного бедствия.

2. Действия в случае несанкционированного доступа к оборудованию

При возникновении ситуации работник обязан:

- сообщить непосредственному руководителю и администратору безопасности;
- принять меры по сохранности свидетельств взлома, несанкционированного проникновения и/или получения доступа к оборудованию ИСПДн МЖКХиТЭК;
- по прибытию администратора безопасности действовать по его указаниям.

При получении сообщения по факту получения несанкционированного доступа к оборудованию ИСПДн МЖКХиТЭК администратор безопасности сообщает о случившемся ответственному за обеспечение информационной безопасности ИСПДн МЖКХиТЭК и обеспечивает выполнение мер обеспечения сохранности свидетельств: взлома, несанкционированного проникновения и/или получения доступа к оборудованию ИСПДн МЖКХиТЭК до прибытия представителей правоохранительных органов.

3. Действия в случае сбоя в работе программного обеспечения

В случае обнаружения программного конфликта между используемыми в ИСПДн МЖКХиТЭК программными средствами работник обязан:

- сообщить непосредственному руководителю и администратору безопасности;
- принять меры по недопущению распространения выявленного программного конфликта на другие средства обработки и защиты информации;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- оказывать помощь администратору безопасности.

Администратор безопасности совместно с соответствующими системными администраторами выясняют причину программного конфликта (сбоя в работе программного обеспечения). Если исправить ситуацию своими силами (в том числе после консультации с разработчиками программного обеспечения) не удалось, составляется акт проверки работоспособности средств и систем ИСПДн МЖКХиТЭК, в среде функционирования которых данный конфликт был обнаружен, копия которого и сопроводительные материалы, свидетельствующие о наличии данной проблемы, направляются разработчикам программного обеспечения.

4. Действия в случае отключения электричества

В случае внешнего отключения электричества администратор безопасности совместно с соответствующими системными администраторами проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования ИСПДн МЖКХиТЭК. В случае необходимости производятся работы по восстановлению последней резервной копии с составлением акта.

5. Действия в случае сбоя в работе оборудования

В случае обнаружения сбоя в работе оборудования работник обязан:

- сообщить непосредственному руководителю и администратору безопасности;
- оказывать помощь администратору безопасности.

По факту выявленного сбоя в работе оборудования ИСПДн МЖКХиТЭК администратор безопасности совместно с системным администратором принимает меры по выводу из эксплуатации дефектного оборудования, проводят анализ состояния данных и (или) установленного программного обеспечения. А при необходимости переносят информацию, хранимую на подверженном сбоям оборудовании, на другой сервер или иное оборудование ИСПДн МЖКХиТЭК.

По факту выявленного сбоя оборудования ИСПДн МЖКХиТЭК составляется акт проверки работоспособности, обосновывающий необходимость проведения работ по его восстановлению.

6. Действия в случае выхода из строя серверного и иного оборудования

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

В случае выхода из строя серверного и иного оборудования ИСПДн МЖКХиТЭК, администратор безопасности совместно с системным администратором, ответственным за эксплуатацию данного оборудования:

- принимают меры по немедленному вводу в действие резервного оборудования;
- проводят оценку технического состояния вышедшего из строя оборудования и составляют акт проверки его работоспособности, с последующей передачей его уполномоченному лицу, ответственному за организацию ремонтно-восстановительных работ в ИСПДн МЖКХиТЭК.

В случае восстановления работоспособности вышедшего из строя оборудования силами обслуживающего персонала должны быть проведены работы по восстановлению программного обеспечения и данных из резервных копий, а также тестирование данного оборудования в условиях близких к реальным.

7. Действия в случае потери данных

При обнаружении потери данных администратор безопасности совместно с системным администратором, ответственным за функционирование программных и программно-технических средств, в среде функционирования которых произошла потеря данных, проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, проверка целостности и работоспособности программного обеспечения и оборудования). По результатам выполненных работ администратором безопасности разрабатываются и направляются в адрес ответственного за обеспечение информационной безопасности информации в ИСПДн МЖКХиТЭК предложения по устранению причин возможной потери данных в дальнейшем. Потерянные данные восстанавливаются из резервных копий с составлением акта восстановления.

8. Действия в случае обнаружения вредоносной программы

В случае обнаружения проявлений вредоносной программы в работе рабочей станции или сервера ИСПДн МЖКХиТЭК необходимо:

- сообщить непосредственному руководителю и администратору безопасности;
- отсоединить «заражённый» сервер или рабочую станцию от ЛВС ИСПДн МЖКХиТЭК;
- оказывать помощь администратору безопасности.

Администратор безопасности совместно с системным администратором, ответственным за обслуживание «зараженного» сервера или рабочей станции, должны провести детальный

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
анализ состояния программно-аппаратной среды и принять меры по восстановлению работоспособности «зараженного» сервера или рабочей станции.

В случае обнаружения фактов проявлений вредоносного кода необходимо:

- приостановить работу зараженного средства обработки информации;
- по возможности физически отключить зараженное средство обработки информации от ЛВС;
- провести лечение или уничтожение зараженных файлов (при необходимости привлечь специалистов);
- в случае обнаружения вредоносной программы, неподдающейся лечению применяемыми антивирусными средствами, сохранить зараженный файл на съемном носителе для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- после ликвидации последствий вирусной атаки, провести внеочередную антивирусную проверку на всем оборудовании ИСПДн МЖКХиТЭК с применением обновлённых антивирусных баз.

О факте обнаружения зараженных файлов администратор безопасности служебной запиской докладывает ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК с указанием предположительного источника (отправителя) зараженного файла, его типа, характера содержащейся в файле информации, типа вредоносной программы, проведенных антивирусных мероприятий и их результатах.

9. Действия в случае обнаружение утечки информации

В качестве основных свидетельств, подтверждающих наличие «скрытых» каналов утечки информации с использованием программных средств должны рассматриваться:

- факты установки несанкционированного программного обеспечения;
- несоответствие конфигураций сетевого оборудования требованиям к маршрутизации и фильтрации сетевого трафика;
- неправомерный доступ к неконтролируемым ресурсам сети Интернет;
- наличие на рабочих станциях и серверах информационных массивов с информацией для обработки, хранения и передачи которой данные СВТ не предназначены;
- обнаружение фактов несанкционированного применения сетевых протоколов.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

В случае обнаружения фактов, подтверждающих наличие «скрытых» каналов утечки информации работнику необходимо:

- сообщить непосредственному руководителю и администратору безопасности;
- действовать по указаниям администратор безопасности.

Работнику, обнаружившему факт наличия «скрытого» канала утечки информации, запрещается без разрешения администратора безопасности сообщать третьим лицам.

Администратор безопасности:

- сообщает об этом ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК;
- проводит предварительный анализ возможностей нарушителя по передаче информации с использованием «скрытого» канала утечки информации;
- докладывает результаты проведенного анализа ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

Ответственный за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК:

- принимает решение по привлечению специалистов, необходимых для проведения анализа возможностей использования «скрытого» канала утечки информации;
- совместно с администратором безопасности и привлеченными специалистами проводит оценку возможностей нарушителя по нанесению материального и/или морального ущерба субъектам персональных данных и Министерству, как оператору персональных данных, обрабатываемых в ИСПДн МЖКХиТЭК, а также свидетелств, документально подтверждающих фактическое нарушение требований политики информационной безопасности;
- на основании результатов детальной оценки принимается один из двух вариантов мер:

1 вариант – ведение наблюдения за нарушителем с целью сбора необходимых доказательств, подтверждающих виновность нарушителя с последующим принятием мер по немедленному блокированию выявленного канала утечки информации, отстранению нарушителя от работы с ресурсами ИСПДн МЖКХиТЭК и проведению служебного расследования;

2 вариант – является разновидностью 1 варианта, при этом наблюдение за нарушителем не проводится, с сразу принимаются меры по блокированию выявленного канала утечки

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ
информации, отстранению нарушителя от работы с ресурсами ИСПДн МЖКХиТЭК и проведению служебного расследования.

10. Действия в случае несанкционированного доступа

По выявленному факту несанкционированного доступа необходимо:

- сообщить непосредственному руководителю и администратору безопасности;
- действовать по указаниям администратор безопасности.

Работнику, обнаружившему взлом системы, запрещается без разрешения администратора сообщать об этом кому бы то ни было.

Администратор безопасности:

- сообщает о факте ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК;
- принимает меры по локализации оборудования, в программно-аппаратной среде которого выявлен факт взлома;
- совместно с системными администраторами проводит ревизию всего программного обеспечения и контроль целостности информационных ресурсов данного средства, на предмет выявления всех свидетельств реализации атаки;
- проводит внеплановую антивирусную проверку, контроль целостности файловой системы, а также иные мероприятия, целесообразность которых определяется по выявленным «следам» взлома;
- при необходимости выполняется восстановление работоспособности системы, включая установленные в ней средства защиты информации;
- совместно с системными администраторами проводит анализ условий и предпосылок несанкционированного проникновения в систему, результаты которого докладывает ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК.

По решению ответственного за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК проводится выборочная или полная проверка применяемых в ИСПДн МЖКХиТЭК мер и средств защиты от несанкционированного доступа.

11. Действия в случае компрометации пароля

В случае выявления факта компрометации пароля (аутентификационной информации субъекта доступа) необходимо:

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- сообщить непосредственному руководителю и администратору безопасности;
- действовать по указаниям администратора безопасности.

Администратор безопасности:

- сообщает о факте ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК;
- совместно с системными администратором, ответственным за обслуживание и сопровождение программных или программно-технических средства и систем, в которых использовалась учетная запись с компрометированным паролем, принимает меры по ее блокированию;
- проводит расследование факта компрометации пароля с целью определения условий и причин ее возникновения;
- в случае отсутствия вины субъекта доступа в компрометации используемого им пароля дает разрешение на предоставление ему необходимых прав доступа в соответствии с установленным регламентом;
- в течение месяца с момента компрометации пароля, ведет контроль попыток использования учетной записи субъекта доступа, заблокированной по факту компрометации пароля, на предмет выявления потенциального нарушителя, использующего возможность получения доступа под правами зарегистрированного пользователя;
- в случае обнаружения потенциального нарушителя, использующего ранее заблокированную учетную запись, действует в соответствии с правилами реагирования на попытку получения несанкционированного доступа к ресурсам ИСПДн МЖКХиТЭК;
- при наличии свидетельств, подтверждающих причастность субъекта доступа в компрометации используемого им пароля, докладывает обстоятельства происшествия ответственному за обеспечение информационной безопасности в ИСПДн МЖКХиТЭК и действует по его указаниям.

Приложение 5
Пример договора о соблюдении
конфиденциальности переданных
персональных данных

Договор № ____

О соблюдении конфиденциальности персональных данных
(проект)

г. Великий Новгород

" ____ " _____ 20__ г.

Министерство жилищно-коммунального хозяйства и топливно-энергетического комплекса, именуемое в дальнейшем «Передающая Сторона», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Получающая Сторона», в лице _____, действующего на основании _____, с другой стороны, далее именуемые «Стороны», с соблюдением требований Федерального закона от 01.11.2006 г. № 152-ФЗ «О персональных данных» заключили настоящий Договор о нижеследующем:

1. Для целей настоящего Договора:

Термин «персональные данные» означает любую информацию Передающей Стороны, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, паспортные данные, ИНН, СНИЛС, номер ОМС и другая предоставляемая информация, которая передается в информационную систему персональных данных Получающей Стороны.

Термин «конфиденциальность информации» означает обязательное для выполнения Получающей стороной требование не передавать полученные от Передающей Стороны персональные данные субъектов третьим лицам без согласия их обладателя.

Информация не подлежит конфиденциальности в случае, если такая информация:

- является или становится общеизвестной не в результате нарушения настоящего Договора;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

- получена Получающей Стороной от третьих лиц, в отношении которых у Получающей Стороны не было сведений о неправомерном раскрытии такими лицами данной информации.

Персональные данные субъектов не могут без предварительного письменного разрешения Передающей Стороны копироваться или иным образом воспроизводиться Получающей Стороной.

2. Передача Передающей Стороной персональных данных субъектов Получающей Стороне может осуществляться письменно, устно или путем передачи (предоставления) персональных данных субъектов на машинных носителях (CD, DVD, flash и т.д.), мультимедийными средствами или в виде фотографий или другими способами.

Передача персональных данных субъектов по настоящему Договору оформляется двусторонним актом, подписываемым представителями Сторон, с указанием количества информации, ее носителя, объема, формата и других идентификационных признаков.

В случае передачи персональных данных субъектов устно или визуально на переговорах либо совещаниях между Сторонами настоящего Договора, ее передача фиксируется путем подписания представителями Сторон соответствующего протокола, с указанием характера персональных данных субъектов, ее объема, формата и других идентификационных признаков.

3. Настоящий Договор не предоставляет Получающей Стороне никаких прав в отношении персональных данных субъектов кроме права использования, необходимого для целей

(указать в каких целях будет использоваться передаваемая информации)

4. В отношении персональных данных субъектов Получающая Сторона обязуется:

4.1. Не использовать персональных данных субъектов в каких-либо других целях, кроме как для целей, определенных в пункте 3 Договора;

4.2. Принимать меры по охране персональных данных субъектов, находящейся на хранении или используемой ею, с такой же степенью, с какой она охраняет собственные персональные данные;

4.3. Раскрывать полученные персональные данные субъектов своим сотрудникам, которым требуется получение такой информации только в тех пределах, которые необходимы для целей, определенных в пункте 3 Договора, соответственно проинформировав их о конфиденциальном характере информации и ограничениях, связанных с ее использованием, а равно иным способом обеспечив соблюдение конфиденциальности информации;

4.4. Раскрывать полученные персональные данные субъектов третьим лицам только при условии получения предварительного письменного согласия Передающей Стороны на такое раскрытие. При этом Передающая Сторона вправе заключить с одобренными ею третьими лицами отдельные соглашения о конфиденциальности в отношении персональных данных субъектов;

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

4.5. По требованию Передающей Стороны возвратить ей или уничтожить персональные данные субъектов, которые были получены Получающей Стороной в течение срока действия настоящего Договора и находится у Получающей Стороны на момент получения соответствующего требования Передающей Стороны.

5. Получающая Сторона имеет право без предварительного письменного согласия Передающей Стороны предоставлять персональные данные субъектов тем лицам, раскрытие информации, в пользу которых, предусмотрено требованиями действующего законодательства, включая любое предписание уполномоченного государственного или судебного органа и только в порядке, установленном таким документом. В случае раскрытия персональных данных субъектов на основании настоящего пункта Получающая сторона ограничит передачу информации запрашиваемым объемом и проинформирует Передающую сторону о факте получения запроса о предоставлении информации в максимально короткие сроки.

6. После окончания действия настоящего Договора либо в случае реорганизации или ликвидации Получающей Стороны, Получающая Сторона обязуется незамедлительно уничтожить или, по просьбе Передающей Стороны, вернуть всю полученную информацию и копии, сделанные с нее.

7. Все споры и разногласия, возникающие в связи с исполнением настоящего Договора, Стороны будут разрешать путем переговоров, а достигнутые договоренности оформлять в виде дополнительных соглашений, подписанных Сторонами и скрепленных печатями. В случае невозможности разрешения споров путем переговоров стороны передают их на рассмотрение в Арбитражный суд Воронежской области.

8. В случае нарушения Получающей Стороной положений настоящего Договора, Получающая Сторона компенсирует все убытки Передающей Стороны, вызванные таким нарушением.

9. В случае признания не действительным или невозможным исполнение любого положения настоящего Договора полностью или частично по любой причине остальные положения настоящего Договора сохраняют юридическую силу и действие в полном объеме настолько, насколько это позволяет действующее законодательство.

10. Все изменения и дополнения к настоящему Договору действительны лишь в случае, если они совершены в письменной форме и подписаны надлежаще уполномоченными представителями Сторон.

11. Настоящий Договор вступает в силу с даты его подписания, действует по «____» _____ 20__ года

12. Настоящий Договор может быть расторгнут по договоренности Сторон либо по инициативе одной из Сторон с предупреждением в письменной форме другой Стороны не менее чем за 30 календарных дней до расторжения настоящего Договора.

13. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

МИНИСТЕРСТВО ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА И ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА НОВГОРОДСКОЙ ОБЛАСТИ

Адреса и реквизиты Сторон

| | |
|--------------------|--------------------|
| Юридический адрес: | Юридический адрес: |
| Фактический адрес: | Фактический адрес: |
| ОГРН: | ОГРН: |
| ИНН: | ИНН: |
| КПП: | КПП: |
| Телефон: | Телефон: |
| Факс: | Факс: |
| Электронный адрес: | Электронный адрес: |

| | | | |
|-------------------|------|-------------------|------|
| Инициалы, фамилия | дата | Инициалы, фамилия | дата |
|-------------------|------|-------------------|------|

М.П.

М.П.