АДМИНИСТРАЦИЯ
ПРИСТЕНСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 30 мая 2024г № 310-па

п. Пристень

Об утверждении инструкции по защите конфиденциальной информации в информационных системах Администрации Пристенского района Курской области

Во исполнение приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Администрация Пристенского района Курской области ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую инструкцию по защите конфиденциальной информации в информационных системах Администрации Пристенского района Курской области (далее – Инструкция).

2. Руководителям структурных подразделений Администрации Пристенского района Курской области и подведомственных учреждений организовать работу по обеспечению безопасности конфиденциальной информации в соответствии с требованиями Инструкции.

3. Признать утратившим силу Постановление Администрации Пристенского района Курской области от 18 мая 2021 № 282 – па «Об утверждении инструкции по защите конфиденциальной информации в информационных системах Администрации Пристенского района Курской области».

4. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации, управляющего делами Администрации Пристенского района Курской области – В.В. Катыхина.

5. Постановление вступает в силу со дня его подписания.

Глава Пристенского района
Курской области **В.В. Петров**

УТВЕРЖДЕНА
постановлением Администрации
Пристенского района
Курской области
от 30.05.2024 № 310-пг

Инструкция по защите конфиденциальной информации в информационных системах Администрации Пристенского района Курской области

1. Термины, определения и сокращения

1.1. Термины и определения

В настоящей Инструкции по защите конфиденциальной информации в информационных системах Администрации Пристенского района Курской области используются следующие основные термины и определения:

1. Автоматизированное рабочее место - комплекс средств вычислительной техники и программного обеспечения, располагающийся непосредственно на рабочем месте сотрудника и предназначенный для автоматизации его работы.

2. Государственная информационная система Курской области - это внешнеориентированная информационная система Курской области, предполагающая участие в сборе и обработке информации, доступа к ней органов исполнительной власти Курской области, органов местного самоуправления, граждан, организаций в соответствии с федеральным законодательством и законодательством Курской области, созданная на основании правового акта государственного органа, в том числе органа государственной власти Курской области, в целях реализации полномочий региональных государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

3. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

4. Информационная система персональных данных - 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.

5. Конфиденциальная информация - документированная информация с ограниченным доступом, не содержащая сведений, составляющих

государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и распоряжением Губернатора Курской области от 17.05.2012 № 360-рг «Об утверждении Перечня сведений конфиденциального характера».

6. Оператор информационной системы – администрация Пристенского района Курской области и его подведомственные организации, сторонняя организация, заключившая соответствующий договор, сотрудники которого осуществляют деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

7. Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу (субъекту персональных данных).

8. Система зашиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

9. Средства защиты информации программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

10. Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

1.2 Принятые сокращения

1.2.1. ИС - информационная система.
1.2.2. ПДн - персональные данные.
1.2.3. ИСПДн - информационная система персональных данных.
1.2.4. ГИС - государственная информационная система.
1.2.5. ОИВ - органы исполнительной власти Курской области.
1.2.6. МНИ - машинный носитель информации.
1.2.7. АРМ - автоматизированное рабочее место.
1.2.8. ПО - программное обеспечение.
1.2.9. СЗИ - система защиты информации.
1.2.10. УБИ- угрозы безопасности информации.
1.2.11. ОРД - организационно-распорядительная документация.
1.2.12. ТЗ - техническое задание.
1.2.13. НСД - несанкционированный доступ.
1.2.14. Инструкция - Инструкция по защите конфиденциальной информации в информационных системах Администрации Пристенского района Курской области.
1.2.15. Комитет - комитет цифрового развития и связи Курской области.

2. Общее положение

Настоящая Инструкция предназначена для организации и проведения работ по обеспечению безопасности защищаемой информации в ИС (ГИС, ИСПДн и ИС, содержащие сведения для служебного пользования). К защищаемой информации относятся ПДн и конфиденциальная информация.

2.1. Цель и задачи зашиты информации в информационных системах органов исполнительной власти Курской области

Целью защиты конфиденциальной информации является предотвращение утечки, хищения, утраты и искажения информации, ее уничтожения, блокирования, модификации и копирования лицами, не имеющими на это права и других форм вмешательства в ИС, а также установление порядка организации и проведения работ но обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну в ИС на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

Задачами защиты конфиденциальной информации являются: выявление возможных каналов утечки информации; предотвращение или существенное затруднение несанкционированного доступа к конфиденциальной информации;

оценка возможностей технических средств разведки и реальной опасности утечки конфиденциальной информации;

предотвращение утечки информации по техническим каналам;

разработка и осуществление экономически обоснованных технических и организационных мероприятий по защите информации;

соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности и достоверности информации в системах ее обработки;

сохранение возможности управления процессом обработки и пользования конфиденциальной информацией;

организация контроля над состоянием защиты информации.

2.2. Нормативно-методическое обеспечение

1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
3. Постановление Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными

правовыми актами, операторами, являющимися государственными или муниципальными органами».

4. Постановление Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» (далее - постановление Правительства Российской Федерации от 6 июля 2015 г. № 676).

6. Приказ ФАПСИ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

7. Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - приказ ФСТЭК России от 11 февраля 2013 года № 17).

8. Приказ ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9. Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости».

10. ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601).

11. ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

12. ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем».

13. ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

14. ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения» (далее - ГОСТ 51583).

15. ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования» (далее - ГОСТ 51624).

16. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России от 14 февраля 2008 года.

17. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК России от 15 февраля 2008 года.

18. Постановление Губернатора Курской области от 05.08.2009 № 252
«О Положении о реестре и паспортах информационных систем Курской области».

19. Распоряжение Администрации Курской области от 30.08.2018 № 347-ра «Об утверждении Основных направлений политики информационной безопасности органов исполнительной власти Курской области».

3. Порядок создания, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации систем защиты информации

3.1. Формирование требований к защите информации в информационных системах

Определение требований к СЗИ, содержащейся в ИС, осуществляется руководителем или ответственными лицами, назначенными руководителем Администрации Пристенского района Курской области, и включает:

принятие решения о необходимости защиты информации, содержащейся в ИС;

классификацию ИС по требованиям защиты информации, определение уровня защищенности ПДн при их обработке в ИС;

определение УБИ, реализация которых может привести к нарушению безопасности информации в ИС, и разработку на их основе модели угроз безопасности информации;

определение требований к СЗИ.

При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

анализ целей создания ИС и задач, решаемых этой ИС;

определение информации, подлежащей обработке в ИС;

анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

принятие решения о необходимости создания СЗИ, а также определение целей и задач защиты информации в ИС, основных этапов создания СЗИ и функций по обеспечению защиты информации, содержащейся в ИС.

При классификации ИС результат оформляется актом классификации ИС.

Результаты определения уровня защищенности ПДн при их обработке в ИС оформляются актом определения уровня защищенности.

УБИ определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации УБИ и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения УБИ используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

По результатам определения УБИ при необходимости разрабатываются рекомендации по корректировке характеристик ИС, направленные на блокирование (нейтрализацию) отдельных УБИ

В модель угроз безопасности информации входит описание ИС и ее характеристик, а также описание УБИ, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИС, способов реализации УБИ и последствий от нарушения свойств безопасности информации.

Требования к СЗИ определяются в зависимости от класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС и УБИ, включенных в модель угроз безопасности информации.

3.2. Разработка системы защиты информации

Разработка СЗИ ИС осуществляется в соответствии с ТЗ на создание ИС и (или) ТЗ на создание СЗИ ИС с учетом модели угроз безопасности информации, предусмотренной подпунктом «г» пункта 1(2) Требований к порядку создания развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 года № 676, ГОСТ 34.601, ГОСТ 51583 и ГОСТ 51624 и, в том числе, включает:

проектирование СЗИ;

разработку эксплуатационной документации на СЗИ;

макетирование (при необходимости) и тестирование СЗИ.

Разработка СЗИ может осуществляться как собственным подразделением (специалистом) по защите информации при взаимодействии и под методическим руководством Комитета, так и

специализированными организациями, имеющими лицензии на этот вид деятельности, на договорной основе.

СЗИ не должна препятствовать достижению целей создания ИС и ее функционированию. При разработке СЗИ учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

При проектировании СЗИ осуществляются следующие мероприятия:

1) определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным ПО, иные объекты доступа);

2) определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в ИС;

3) выбираются меры защиты информации, подлежащие реализации в СЗИ;

4) определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

5) определяется структура СЗИ, включая состав (количество) и места размещения ее элементов;

6) осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС;

7) определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению УБИ;

8) определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

ТЗ формируется в соответствии с подпунктами «а» и «в» пункта 1(1) Требований к порядку создания развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 года № 676, с учетом требований к защите информации, содержащейся в ИС.

Перед отправкой в Управление ФСТЭК по Центральному федеральному округу модель угроз безопасности информации ГИС и (или) ТЗ на создание ГИС согласуется с Комитетом, в пределах его полномочий в части, касающейся выполнения установленных требований о защите информации.

Для разработки модели угроз безопасности информации администрация Пристенского района Курской области может использовать Типовую модель угроз безопасности информационных систем персональных данных органов государственной власти Курской области, утвержденную Комиссией по информационной безопасности при Губернаторе Курской области,

Макетирование (при необходимости) и тестирование СЗИ производится для проверки работоспособности и совместимости средств защиты информации, выполнения соответствующих требований к СЗИ и (или) корректировки проектных решений по созданию СЗИ ИС.

ТЗ на создание СЗИ ИС и модель угроз безопасности информации утверждаются руководителем Администрации Пристенского района Курской области или его заместителем, ответственным за организацию по созданию СЗИ ИС.

3.3. Внедрение системы зашиты информации

Внедрение СЗИ организуется в соответствии с проектной и эксплуатационной документацией на СЗИ и, в том числе, включает:

1) установку и настройку СЗИ в ИС;
2) разработку ОРД, определяющей правила и процедуры, реализуемые администрацией Пристенского района Курской области для обеспечения защиты информации в ИС в ходе ее эксплуатации;
3) внедрение организационных мер защиты информации;
4) предварительные испытания СЗИ (при необходимости);
5) опытную эксплуатацию СЗИ (при необходимости);
6) анализ уязвимостей ИС и принятие мер защиты информации по их устранению;
7) приемочные испытания СЗИ' (при необходимости).

Установка и настройка средств защиты информации в ИС проводится в соответствии с эксплуатационной документацией на СЗИ и документацией на средства зашиты информации.

Разрабатываемая ОРД по защите информации определяет правила и процедуры:

1) планирования мероприятий по защите информации в ИС;
2) выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению УБИ, и реагирования на них;
3) управления конфигурацией арестованной ПС и СЗИ;

4) контроля за обеспечением уровня защищенности информации, содержащейся в ИС;

5) информирования и обучения персонала ИС;

6) защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

При внедрении организационных мер защиты информации осуществляются:

1) реализация правил разграничения доступа (матрица доступа), регламентирующих права доступа субъектов доступа к объектам доступа, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения и введение ограничений на действия пользователей;

2) проверка полноты и детальности описания в ОРД по защите информации действий пользователей и администраторов ИС по реализации организационных мер защиты информации;

3) отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

Предварительные испытания СЗИ включают проверку работоспособности СЗИ, а также принятие решения о возможности опытной эксплуатации СЗИ.

Опытная эксплуатация СЗИ включает проверку функционирования СЗИ, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации СЗИ.

Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации УБИ. Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и ПО ИС. При анализе уязвимостей ИС проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и ПО, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и ПО, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и ПО. В случае выявления уязвимостей ИС, приводящих к возникновению дополнительных УБИ, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность

использования нарушителем выявленных уязвимостей. По результатам анализа уязвимостей должно быть подтверждено, что в ИС отсутствуют уязвимости, содержащиеся в банке данных УБИ ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

Приемочные испытания СЗИ ИС включают проверку выполнения требований к СЗИ ИС в соответствии с ТЗ на создание СЗИ ИС.

3.4. Аттестация информационной системы

Аттестация ИС организуется руководителем Администрации Пристенского района Курской области или, по решению руководителя Администрации Пристенского района Курской области, администратором безопасности ИС и (или) ответственным за организацию обработки ПДн в ИС, и включает проведение комплекса аттестационных испытаний, в результате которых подтверждается соответствие СЗИ ИС с ТЗ на создание СЗИ ИС и модели угроз безопасности информации ИС.

Аттестат соответствия выдается на весь срок эксплуатации СЗИ ИС, в соответствии с приказом ФСТЭК России от 11.02.2013 № 17. Администратор безопасности информации ИС в ходе эксплуатации ИС обеспечивает поддержку соответствия СЗИ аттестату соответствия в рамках реализации мероприятий, предусмотренных настоящей Инструкцией.

Повторная аттестация (переаттестация) ИС осуществляется по окончании срока действия сертификатов средств защиты информации, изменении класса защищенности ИС или других изменений в СЗИ ИС. При изменении состава УБИ или проектных решений, реализованных при создании СЗИ, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Ввод в эксплуатацию СЗИ ИС осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Губернатора Курской области от 05.08.2009 № 252 «О Положении о реестре и паспортах информационных систем Курской области» и при наличии аттестата соответствия.

3.5. Обеспечение защиты информации в ходе эксплуатации

Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется администратором безопасности информации ИС, в соответствии с эксплуатационной документацией на СЗИ и ОРД по защите информации и в том числе включает:

1) планирование и контроль мероприятий по защите информации в ИС;
2) анализ УБИ в ИС;
3) управление (администрирование) СЗИ;
4) выявление инцидентов и реагирование на них;
5) управление конфигурацией ИС и ее СЗИ;
6) информирование и обучение персонала ИС;
7) контроль за обеспечением уровня защищенности информации, содержащейся в ИС.

В ходе планирования мероприятий по защите информации в ИС осуществляется:

1) определение лиц, ответственных за планирование и контроль мероприятий по защите информации в ИС;

2) определение лиц, ответственных за выявление инцидентов и реагирование на них;

3) разработка, утверждение и актуализация плана мероприятий по защите информации в ИС;

4) определение порядка контроля выполнения мероприятий по защите информации в ИС, предусмотренных утвержденным планом.

Планирование мероприятий по защите информации в ИС и контроль выполнения мероприятий осуществляются в соответствии с приложением № 4 к настоящей Инструкции.

В ходе анализа УБИ в ИС осуществляется выявление, анализ и устранение известных уязвимостей ИС.

Периодичность проведения указанных работ определяется в плане мероприятий по защите информации.

В ходе управления (администрирования) СЗИ осуществляются:

определение администратора безопасности СЗИ ИС;

управление учетными записями пользователей ИС и поддержание в актуальном состоянии правил разграничения доступа в ИС;

управление средствами защиты информации в ИС;

управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС;

обеспечение функционирования СЗИ в ходе ее эксплуатации, включая ведение эксплуатационной документации и ОРД по защите информации.

В ходе выявления инцидентов и реагирования на них осуществляются:

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, ПО и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование операторами ИС и администраторами ИС лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также опенка их последствий;

планирование и принятие мер по устранению и повторному возникновению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных

программ (вирусов) и иных событии, приводящих к возникновению инцидентов, руководствуясь приложением № 5 к настоящей Инструкции.

В ходе управления конфигурацией ИС и ее СЗИ осуществляются:

1) определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и ее СЗИ, их полномочия;

2) определение компонентов ИС и ее СЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

3) управление изменениями ИС и ее СЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на защиту информации, санкционирование внесения изменений в ИС и ее СЗИ, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации ИС;

4) контроль действий по внесению изменений в ИС и ее СЗИ.

В ходе информирования и обучения персонала ИС осуществляются:

1) информирование персонала ИС о появлении актуальных УБИ, о правилах безопасной эксплуатации ИС;

2) доведение до персонала ИС требований по защите информации, а также положений ОРД по защите информации с учетом внесенных в них изменений;

3) обучение персонала ИС правилам эксплуатации отдельных средств защиты информации и блокированию УБИ и реагированию на инциденты.

В ходе контроля за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

1) контроль (анализ) защищенности информации с учетом особенностей функционирования ИС;

2) анализ и оценка функционирования ИС и ее СЗИ, включая анализ и устранение уязвимостей и иных недостатков в функционировании СЗИ;

3) документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в ИС;

4) принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в ИС, о необходимости доработки (модернизации) ее СЗИ.

Регулярные мероприятия по обеспечению безопасности защищаемой информации проводятся в соответствии с планом мероприятий по защите информации. Внутренние проверки режима защиты информации проводятся в соответствии с планом внутренних проверок режима защиты информации. По результатам проведения внутренней проверки составляется акт (справка) с результатами внутренней проверки режима защиты информации в ОИВ.

3.6. Обеспечение защиты информации при выводе из эксплуатации или после принятия решения об окончании обработки информации в информационной системе

3.6.1. Общие положения

Настоящая инструкция предназначена для обеспечения защиты информации при выводе из эксплуатации или после принятия решения об окончании обработки информации в информационных системах Администрации Пристенского района Курской области.

3.6.2. Порядок организации

1. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором информационной системы, в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации, и в том числе включает:

– архивирование информации, содержащейся в информационной системе;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора информационной системы.

3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации на информационной системе, производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется гарантированная очистка (стирание) данных с этих машинных носителей информации в соответствии с утвержденным Порядком обращения, хранения и уничтожения машинных носителей защищаемой информации в информационной системе.

При выводе из эксплуатации элементов информационной системы, содержащих оптические носители информации (CD-дисков), используемые для хранения и обработки информации, осуществляется физическое уничтожение этих оптических носителей информации в соответствии с утвержденным порядком обращения, хранения и

уничтожения машинных носителей информации в информационной системе.

3.6.3. Ответственность

Ответственность за соблюдение требований по обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации возлагается на оператора.

4. Мероприятия по защите конфиденциальной информации Администрации Пристенского района Курской области

4.1. Мероприятия по защите конфиденциальной информации

В целях зашиты информации в ИС проводятся правовые, организационные, программно-технические, технические, специальные (криптографические) и другие мероприятия.

Правовые мероприятия предусматривают разработку ОРД в соответствии с пунктом 4.2 настоящей Инструкции.

Организационные мероприятия предусматривают:

1) назначение ответственного за организацию обработки ПДн (в должности не ниже заместителя руководителя), типовые обязанности которого приведены в приложении № 1 к настоящей Инструкции;

2) назначение администратора безопасности информации в ИС, типовые обязанности которого приведены в приложении № 2 к настоящей Инструкции;

3) назначение пользователей ПДн, типовые обязанности которых приведены в приложении № 3 к настоящей Инструкции;

4) подбор и подготовку кадров для работы в ИС;

5) повышение квалификации работников, обеспечивающих безопасность информации, в соответствии с постановлением Правительства Российской Федерации от 06 мая 2016 г. № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»;

6) осуществление постоянного контроля над процессом обработки защищаемой информации.

Программно-технические и технические мероприятия обеспечивают:

1) создание СЗИ в соответствии с ТЗ на создание ИС и (или) ТЗ на создание СЗИ ИС с учетом модели угроз безопасности информации, сформированные в соответствии с пунктом 3.1 настоящей Инструкции;

2) проведение мероприятий по защите информации в ИС;

3) предотвращение утечки обрабатываемой информации путем исключения НСД;

4) предотвращение специальных воздействий, вызывающих разрушение, уничтожение, искажение информации;

5) выявление внедренных программных или аппаратных закладочных устройств;

6) предотвращение перехвата информации, распространяющейся по техническим каналам, путем их выявления и локализации.

4.2. Рекомендованный перечень организационно-распорядительной документации

1. Модель угроз безопасности информации.
2. Техническое задание на создание СЗИ ИС.
3. Приказ о назначении лиц, ответственных за обеспечение безопасности ПДн в ИС.
4. Функциональные обязанности администратора безопасности информации в ИС.
5. Приказ об определении перечня помещений, предназначенных для обработки защищаемой информации в ИС, и организации режима обеспечения безопасности в них.
6. Перечень лиц, имеющих доступ в кабинет, в котором обрабатывается защищаемая информация, в том числе ПДн.
7. Список лиц, допущенных к работе в ИС.
8. Перечень лиц, доступ которых к ПДн, подлежащим обработке в ИСПДн в составе ИС, необходим для выполнения ими служебных обязанностей.
9. Перечень защищаемых информационных ресурсов ИС.
10. Технический паспорт ИС.
11. Перечень параметров настройки ПО в ИС.
12. Данные по уровню подготовки кадров, обеспечивающих защиту информации в ИС.
13. Приказ об определении совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определении на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в ИС.
14. Акт определения совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определения на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в ИС в составе ИС.
15. Приказ о классификации ИС.
16. Акт классификации ИС.
17. Инструкция по организации режима обеспечения безопасности помещений ИС.
18. Инструкция о действиях сотрудников при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров! в помещениях ИС.

19. Инструкция администратора безопасности информации в ИС.
20. Инструкция по работе пользователей в ИС.
21. Инструкция по парольной защите.
22. Инструкция по антивирусной защите.
23. Инструкция по учету и маркированию МНИ.
24. Инструкция по обеспечению доступности информации в ИС.
25. Расписка в ознакомлении лиц, доступ которых к информации ограниченного доступа, обрабатываемой в ИС, необходим для выполнения ими своих служебных обязанностей с перечнем и содержанием нормативных правовых актов, в том числе локальных, устанавливающих требования по соблюдению конфиденциальности персональных данных, а также требований по обеспечению безопасности информации ограниченного доступа, в том числе персональных данных, и мер ответственности за их несоблюдение.
26. Порядок хранения, использования и передачи ПДн сотрудников.
27. Документ, определяющий политику в отношении обработки ПДн.
28. Приказ о комиссии по уничтожению защищаемой информации.
29. Приказ об обеспечении безопасности МНИ.
30. Инструкция ответственного за реализацию мер, необходимых для обеспечения сохранности защищаемой информации в части обработки ПДн и исключающих НСД при хранении МНИ.
31. Перечень мест хранения МНИ, содержащих защищаемую информацию.
32. Приказ о назначении ответственного за планирование и контроль мероприятий по защите информации в ИС.
33. Приказ о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них.
34. Приказ о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и СЗИ.
35. Регламент внесения изменений в конфигурацию ИС и СЗИ.
36. Приказ о вводе в эксплуатацию ИС.

5. Планирование мероприятий по защите информации и контролю

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 планирование мероприятий по защите информации в ИС Администрации Пристенского района Курской области является одним из основных мероприятий при обеспечении защиты информации в ходе эксплуатации ИС.

Планирование мероприятий по защите информации включает следующие этапы:

планирование организационных мероприятий (организация разработки и использования документов и носителей защищаемой

информации, их учет, исполнение, организация работ по анализу внутренних и внешних угроз защищаемой информации, обучение сотрудников правилам работы с защищаемой информацией и другое);

планирование контрольных мероприятий (планирование внутренних проверок СЗИ);

планирование мероприятий по созданию СЗИ, которое включает планирование финансирования данных мероприятий.

Финансирование мероприятий по защите информации в Администрации Пристенского района Курской области и их подведомственных организациях осуществляется за счет средств подпрограммы «Развитие системы защиты информации Курской области» государственной программы Курской области «Развитие информационного общества в Курской области», утвержденной постановлением Администрации Курской области от 24.10.2013 № 775-па «Об утверждении государственной программы Курской области «Развитие информационного общества в Курской области», средств Администрации Пристенского района Курской области и их подведомственных организаций, выделяемых на защиту ИС из бюджета Курской области, и федеральных субсидий, выделяемых в рамках региональных проектов.

При планировании проведения мероприятий по защите информации Администрации Пристенского района Курской области, объём финансирования на проведение указанных мероприятий рассчитывается в соответствии с требованиями действующего законодательства.

При планировании мероприятий по защите информации администрация Пристенского района Курской области должна согласовывать их объемы и состав с Комитетом и ежегодно до 1 октября текущего года предоставлять в Комитет перечень запланированных мероприятий по защите информации в Администрации Пристенского района Курской области и их подведомственных учреждениях и объемы финансовых средств, необходимых для реализации указанных мероприятий, в том числе предусмотренных в бюджете Курской области на следующий год.

Планирование работ по защите информации в Администрации Пристенского района Курской области с правами юридического лица осуществляется специалистом по защите информации (администраторами безопасности информации). Планы утверждаются руководителем Администрации Пристенского района Курской области.

По результатам выполнения этих планов в Администрации Пристенского района Курской области составляются годовые отчеты о проделанной работе по защите информации, которые до 15 декабря текущего года направляются в Комитет.

6. Организация контроля за состоянием систем защиты информации

Контроль за состоянием СЗИ заключается в проверке выполнения требований нормативных актов по защите информации, решений ФСТЭК России, приказов ФСБ России, руководящих документов Роскомнадзора, решений и методических рекомендаций Комиссии по информационной безопасности при Губернаторе Курской области, а также в оценке обоснования и эффективности принятых мер по защите информации в Администрации Пристенского района Курской области.

Контроль за состоянием и эффективностью СЗИ организуется и проводится в целях:

своевременного выявления и предотвращения утечки защищаемой информации;

исключения или существенного затруднения НСД к информации, хищения или утраты технических средств и МНИ;

разработки рекомендаций по защите информации в ИС при их эксплуатации.

Организация и проведение контроля - необходимое условие осуществления эффективной защиты конфиденциальной информации. Основными формами контроля защиты конфиденциальной информации являются периодические, плановые и внезапные проверки, обследования объектов, их аттестация, а также организация повседневного контроля.

Плановый и внеплановый внешний контроль осуществляется федеральными органами контроля, а также Комитетом. Периодический внутренний контроль состояния защиты информации в Администрации Пристенского района Курской области осуществляется соответствующими специалистами по защите информации (администраторами безопасности информации).

Контроль состояния защиты конфиденциальной информации федеральными органами осуществляется в установленные ими сроки и в пределах предоставленных полномочий в соответствии с действующим законодательством.

Плановый внешний контроль состояния системы защиты конфиденциальной информации осуществляется Комитетом в соответствии с утвержденными годовыми планами работ.

Периодический внутренний контроль за реализацией мероприятий по информационной безопасности в Администрации Пристенского района Курской области с правами юридического лица осуществляется самостоятельно данными органами. Результаты проведения внутреннего контроля направляются в адрес Комитета не позднее 5 рабочих дней с даты их утверждения.

Периодический внутренний контроль за реализацией мероприятий по информационной безопасности учреждений, подведомственных Администрации Пристенского района Курской области, осуществляется самостоятельно администрацией Пристенского района Курской области.

Типовой план проведения контроля состояния СЗИ в Администрации Пристенского района Курской области представлен в приложении № 4 к

Основным направлениям политики информационной безопасности органов исполнительной власти Курской области, утвержденным распоряжением Администрации Курской области от 30.08.2018 № 347-ра «Об утверждении Основных направлений политики информационной безопасности органов исполнительной власти Курской области».

Внеплановый контроль осуществляется Комитетом при выявлении инцидентов информационной безопасности (признаков утечки защищаемой информации или предпосылок к утечке защищаемой информации) в Администрации Пристенского района Курской области и на основании предписания на проведение контроля без предварительного уведомления объекта контроля.

Руководитель проверенного структурного подразделения в соответствии с полученными материалами о результатах контроля должен провести необходимые мероприятия по устранению выявленных нарушений, о чем в течение 30 календарных дней со дня получения указанных материалов должен проинформировать Комитет.

При обнаружении нарушений руководитель проверенного подразделения обязан организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их возникновения в дальнейшем и привлечения к ответственности виновных лиц, а также устранение выявленных нарушений.

На этане эксплуатации ИС для проверки выполнения требований нормативных документов по защите информации осуществляется периодический внутренний контроль. Периодичность проведения контроля специалистами по защите информации (администраторами безопасности информации) - не реже одного раза в год.

Кроме того, внутренней контроль осуществляется ответственными сотрудниками Администрации Пристенского района Курской области (ответственным за организацию обработки ПДн или администратором безопасности информации) в течение 20 рабочих дней после реконструкции или ремонта помещений, в которых располагаются технические средства ИСПДн.

Защита информации в ИС считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам. Несоответствие принимаемых мер установленным требованиям и нормам ОРД по защите информации является нарушением и влечет наступление ответственности, установленной действующим законодательством.

Приложение № 1
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Типовые обязанности ответственного за организацию обработки персональных данных

1. Основные функции и обязанности лица, ответственного за организацию обработки персональных данных

Функции лица, ответственного за организацию обработки ПДн (далее - Ответственный), заключаются в изучении всех сторон деятельности Администрации Пристенского района Курской области для формирования рекомендаций по организации обработки ПДн с решением ряда основных вопросов:

- организация доступа к ПДн и учет сотрудников Администрации Пристенского района Курской области, допущенных к обработке ПДн как в программных комплексах, входящих в состав информационных систем, так и на бумажных носителях;
- контроль за поддержанием в актуальном состоянии действующих локальных актов, журналов и форм учета по работе с ПДн;
- контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
- организация работы по заключению договоров на работы по защите ПДн;
- контроль за поддержанием в актуальном состоянии уведомления об обработке ПДн;
- рассмотрение предложений по совершенствованию действующей системы защиты ПДн, внесенных Администратором, в ИС Администрации Пристенского района Курской области;
- осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Администрации Пристенского района Курской области.

Обязанности Ответственного:

- знать цели обработки ПДн в ОИВ и перечень обрабатываемых ПДн;
- соблюдать требования документа, определяющего политику в отношении обработки персональных данных в Администрации Пристенского района Курской области, и иных локальных актов Администрации Пристенского района Курской области, устанавливающих порядок работы с ПДн;

- обеспечивать доведение до сведения сотрудников Администрации Пристенского района Курской области нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн, локальных актов Администрации Пристенского района Курской области по вопросам обработки ПДн;

- осуществлять внутренний контроль за соблюдением сотрудниками Администрации Пристенского района Курской области норм действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

- контролировать ведение документации, предусмотренной локальными актами Администрации Пристенского района Курской области в части обеспечения безопасности ПДн;

- обеспечивать доработку локальных актов по защите ПДн Администрации Пристенского района Курской области;

- расследовать нарушения по вопросам защиты информации, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений;

- обеспечивать организацию проведения занятий со специалистами Администрации Пристенского района Курской области по организационным вопросам обработки ПДн (проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в Администрации Пристенского района Курской области);

обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов в соответствии с пунктом 3 части 4 статьи 22.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Права лица, ответственного за организацию обработки персональных данных

Ответственный имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач;

- проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных подразделениях Администрации Пристенского района Курской области (при их наличии);

- требовать от сотрудников Администрации Пристенского района Курской области соблюдения требований документа, определяющего политику в отношении обработки персональных данных в Администрации Пристенского района Курской области, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн;

- требовать от сотрудников Администрации Пристенского района Курской области письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн;

- вносить предложения руководителю Администрации Пристенского района Курской области об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн;

- давать сотрудникам Администрации Пристенского района Курской области обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации, Курской области и требованиями Администрации Пристенского района Курской области;

- привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

3. Ответственность лица, ответственного за организацию обработки персональных данных

Ответственный в соответствии с возложенными на него обязанностями несет ответственность за:

- несоблюдение требований федеральных нормативных правовых актов, нормативных правовых актов Курской области и локальных актов Администрации Пристенского района Курской области, устанавливающих порядок работы с ПДн в пределах, установленных трудовым договором (служебным контрактом);

- разглашение ПДн в соответствии с действующим административным, уголовным и гражданским законодательством Российской Федерации.

Приложение № 2
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации Пристенского
района Курской области

Типовые обязанности администратора безопасности информации

1. Функции и обязанности администратора безопасности информации информационных систем

1.1. Функции администратора безопасности информации (далее - Администратор):

1.1.1. Управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в информационной системе.

1.1.2. Управление средствами защиты информации информационной системы.

1.1.3. Управление обновлениями программных и программно--аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования информационной системы.

1.1.4. Централизованное управление системой защиты информации информационной системы (при необходимости).

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

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

1.2. Администратор обязан:

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

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

1.2.3. Знать состав, структуру и назначение системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов.

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

- исполнение требований по защите информации в соответствии с проектной и организационной - распорядительной документацией на систему защиты информации информационной системы;

- реализацию принятых решений по обеспечению защиты информации, обрабатываемой в информационной системе;

- информирование Ответственного за организацию обработки ПДн о выявленных недостатках по результатам выполнения контрольных мероприятий;

- контроль работ, проводимых сторонними организациями на технических средствах информационной системы;

- неразглашение информации ограниченного доступа, ставшей доступной в ходе исполнения должностных обязанностей.

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

- верификацию (проверку) личности пользователя, его должностных (функциональных) обязанностей при заведении учетной записи пользователя;

- заведение, активацию, блокирование и уничтожение учетных записей пользователей;

- пересмотр и при необходимости корректировку учетных записей пользователей;

- своевременное уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

- реализацию правил разграничения доступа и полномочий пользователей в информационной системе на основе утвержденной руководителем Администрации Пристенского района Курской области системы разграничения доступа;

- контроль правил генерации и смены паролей пользователями информационной системы, реализации правил разграничения доступа, полномочий пользователей в информационной системе;

- устранение нарушений, связанных с генерацией и сменой паролей пользователями, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступа, установлением полномочий пользователей.

1.2.6. В рамках реализации функций управления средствами защиты информации информационной системы обеспечивать:

- корректную эксплуатацию пользователями средств защиты информации;

- консультирование пользователей, участвующих в процессах обработки и обеспечения безопасности информации, по вопросам использования средств защиты информации;

- техническое обслуживание средств защиты информации информационной системы в соответствии с эксплуатационной документацией на средства защиты информации;

- устранение выявленных в средствах защиты информации уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации;

- периодический контроль работоспособности (неотключения) средств защиты информации;

- периодический контроль целостности программного обеспечения средств защиты информации;

- периодический контроль соответствия настроек средств зашиты информации;

- принятие мер по восстановлению работоспособности (правильности функционирования) и параметров настройки средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов, в случае выявления фактов нарушения работоспособности или отклонения параметров настроек средства защиты информации;

- периодический контроль соответствия состава средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;

- периодическое выполнение тестирования функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств;

- периодический контроль состава средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- периодический контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

- исключение из состава информационной системы несанкциониро¬ванно установленных средств защиты информации;

- восстановление несанкционированно удаленных средств защиты информации;

- настройку средств защиты информации, направленную на устранение возможности использования выявленных уязвимостей (при необходимости);

- согласование изменения конфигурации системы зашиты информации и настроек средств защиты информации с Ответственным за организацию обработки ПДн.

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

- получение из доверенных источников и установку обновлений программного обеспечения, включая программное обеспечение средств защиты информации;

- контроль целостности файлов обновлений;

- проверку соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленною в информационной системе и выпущенного разработчиком;

- запись об установке (применении) обновлений в соответствующей эксплуатационной документации;

- обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной зашиты;

- обновление базы решающих правил систем обнаружения вторжений, применяемых в информационной системе (при наличии таковых);

- выполнение обновления программного обеспечения средств зашиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств с целью устранения выявленных уязвимостей.

1.2.8. В рамках реализации функций централизованного управления системой защиты информации информационной системы обеспечивать централизованное управление установкой, удалением, обновлением, конфигурированием и (или) контролем актуальности версий программного обеспечения средств зашиты информации, эксплуатируемых в информационной системе.

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

- регистрацию событий безопасности в соответствии с перечнем событий, подлежащих регистрации в информационной системе;

- периодический просмотр журналов регистрации событий безопасности:

- реагирование на сбои при регистрации событий безопасности;

- оперативное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о попытках и (или) фактах несанкционированного доступа или подозрительных событиях;

- содействие при проведении расследований инцидентов информационной безопасности.

1.2.10. Обеспечивать неразглашение информации о параметрах настройки ПО и СЗИ.

2. Права администратора безопасности информации информационных систем

2.1. Администратор имеет право:

2.1.1. Знакомиться с локальными актами Администрации Пристенского района Курской области, регламентирующими процессы обработки защищаемой информации.

2.1.2. Вносить предложения Ответственному за организацию обработки ПДн по совершенствованию существующей системы защиты информации.

2.1.3. Требовать от пользователей информационных систем соблюдения требований инструкции пользователя информационных систем ОИВ, а также соблюдения требований действующего законодательства Российской Федерации и Курской области в сфере (области) обработки и обеспечения безопасности информации.

2.1.4. Требовать от Ответственного за организацию обработки ПДн оказания содействия в исполнении функций и обязанностей, предусмотренных настоящей Инструкцией.

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

2.1.6. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность информации, вносить свои предложения по совершенствованию организационных и технических мер обеспечения безопасности информации.

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

2.1.8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности информации к Ответственному за организацию обработки ПДн.

3. Ответственность администратора безопасности информации информационных систем

3.1. Администратор несет персональную ответственность:

3.1.1. За работоспособность и надлежащее функционирование системы защиты информации.

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

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

3.1.4. За несоблюдение требований действующего законодательства Российской Федерации и Курской области, локальных актов ОИВ, устанавливающих порядок работы с защищаемой информацией, не содержащей сведения, составляющие государственную тайну, в пределах, установленных трудовым договором (служебным контрактом).

Приложение № 3
к Инструкции по защите
конфиденциальной информации в
информационных системах
Администрации Пристенского района
Курской области

Типовая инструкция пользователя информационной системы

I. Инструкция о порядке работы пользователя в информационных системах Администрации Пристенского района Курской области

1. Общие положения

1.1. Пользователь информационной системы (далее – Пользователь), осуществляет обработку защищаемой информации, в т.ч. персональных данных, в информационной системе Администрации Пристенского района Курской области.

1.2. Пользователем является каждый сотрудник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информационной системы, содержащей защищаемую информацию.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, нормативными документами ФСТЭК России, ФСБ России, регламентирующими документами Администрации и другими документами.

1.5. Методическое руководство работой пользователя в части выполнения положений законодательства Российской Федерации и внутренних документов Администрации в области обеспечения защиты информации осуществляется администратором безопасности информационной системы.

2. Должностные обязанности

Пользователь информационной системы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы, содержащей защищаемую информацию, несет персональную ответственность за свои действия и обязан:

2.1. Решать поставленные задачи в соответствии с полномочиями доступа к ресурсам информационной системы, присвоенными администратором безопасности данному пользователю. При этом для хранения файлов, содержащих конфиденциальные сведения, разрешается

использовать только соответствующим образом учтенные носители информации.

2.2. Знать и выполнять требования, действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

2.3. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.4. Знать и строго выполнять правила работы со средствами защиты информации, установленными в информационной системе.

2.5. Хранить в тайне свой пароль. Периодически менять пароль в соответствии с Инструкцией по организации парольной защиты.

2.6. По окончании работы пользователь обязан произвести стирание остаточной информации на несъемных носителях (жестких дисках) и в оперативной памяти. Одним из способов стирания остаточной информации в оперативной памяти является перезагрузка ПЭВМ.

2.7. В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля немедленно обратиться к администратору безопасности.

2.8. Строго соблюдать требования Инструкции по организации антивирусной защиты. В случае обнаружения вирусов немедленно сообщить об этом администратору безопасности.

2.9. Знать и соблюдать установленные требования по учету, хранению машинных носителей информации.

2.10. Немедленно ставить в известность администратора безопасности и в случае подозрения, а также при обнаружении фактов совершения попыток несанкционированного доступа (далее – НСД) к ресурсам информационной системы:

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств информационной системы;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию информационной системы, выхода из строя или неустойчивого функционирования узлов информационной системы или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– непредусмотренных отводов кабелей и подключенных устройств.

2.11. Для получения консультаций по вопросам работы ПЭВМ и настройке программного обеспечения необходимо обращаться к администратору информационной системы, по вопросам работы средств защиты информации – к администратору безопасности.

2.12. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.13. Пользователям ЗАПРЕЩАЕТСЯ:

– использовать компоненты программного и аппаратного обеспечения информационной системы в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств информационной системы или устанавливать дополнительно любые программные и аппаратные средства;

– осуществлять обработку защищаемой информации, в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить защищаемую информацию (содержащую сведения ограниченного распространения), в т.ч. ПДн, на неучтенных носителях информации;

– оставлять включенной без присмотра рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок ставить в известность администратора безопасности;

– осуществлять какие-либо действия в информационной системе до прохождения процедур идентификации и аутентификации;

– подключать к рабочей станции и вычислительной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– привлекать посторонних лиц для производства ремонта или настройки АРМ;

– разглашать защищаемую информацию третьим лицам;

– копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

3. Правила работы в сетях общего доступа и (или) международного информационного обмена

3.1. Работа в сетях общего доступа и (или) международного информационного обмена (сети Интернет и других) (далее – Сеть) на элементах информационной системы, должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран и других);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– запрещается скачивать из Сети программное обеспечение и другие файлы;

– запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);

– запрещается нецелевое использование подключения к Сети.

4. Права и ответственность пользователей

Пользователь информационной системы имеет право в отведенное ему время решать поставленные задачи в соответствии с его полномочиями к ресурсам информационной системы и вверенным ему техническим и программным средствам.

Пользователь информационной системы, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы, несет персональную ответственность за свои действия.

Также пользователь информационной системы несет ответственность по действующему законодательству за разглашение сведений конфиденциального характера, ставших известными ему по роду работы.

Пользователи, виновные в несоблюдении настоящей Инструкции, расцениваются как нарушители законодательства РФ в области защиты информации и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

II. Инструкция по организации парольной защиты в информационных системах Администрации Пристенского района Курской области

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) при организации доступа в информационные системы Администрации Пристенского района Курской области.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей для доступа к информационной системе, возлагается на администратора безопасности информационной системы (далее – администратор безопасности).

1.3. Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2. Порядок организации парольной защиты

2.1. Личные пароли должны генерироваться и распределяться централизованно администратором безопасности с учетом следующих требований:

– длина пароля должна быть не менее шести символов, алфавит пароля - не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - от 3 до 10 попыток;

– блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - от 5 до 15 минут;

– в числе символов пароля обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

– личный пароль пользователь не имеет права сообщать никому.

2.2. Ответственность за правильность формирования и распределения паролей возлагается на администратора безопасности.

2.3. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 120 дней.

2.4. Время бездействия (неактивности) пользователя до блокирования сеанса доступа пользователя в информационную систему должно составлять не более 15 минут или по запросу пользователя. Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации.

2.5. Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.6. В случае прекращения полномочий администратора безопасности производится полная внеплановая смена всех паролей.

2.7. В случае компрометации личного пароля пользователя системы должны быть немедленно предприняты меры в соответствии с п. 2.4 или п. 2.5. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.8. Использование в информационной системе 2-х последних значений паролей при создании новых паролей не допустимо.

2.9. Хранение пользователем значений своих паролей на бумажном носителе допускается только в опечатанном печатью конверте в сейфе у администратора безопасности.

2.10. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.). Вводимые символы пароля должны отображаться условными знаками «*», «•» или иными знаками.

2.11. Повседневный контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности.

2.12. Временные пароли, заданные при внедрении системы защиты информации информационной системы сотрудниками сторонних организаций, рекомендуется изменить при первом входе в систему.

2.13. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. Ответственность

3.1. Ответственность за соблюдение требований хранения и использования паролей возлагается на их владельца.

3.2. Ответственность за соблюдение требований, а также за своевременное информирование о необходимости смены паролей в подразделении возлагается на администратора безопасности информационной системы.

III. Технология обработки защищаемой информации

1. При первичном допуске к работе с ИС пользователь:

- проходит инструктаж по использованию ИС;
- знакомится с требованиями локальных актов, регламентирующих обработку и обеспечение безопасности защищаемой информации;
- получает у Администратора идентификатор и личный пароль для входа в ИС.

2. Перед началом работы пользователь визуально проверяет целостность АРМ, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

3. В процессе работы на АРМ ИС пользователь использует технические средства и установленное программное обеспечение согласно техническому паспорту ИС.

4. Копирование защищаемой информации на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

5. При необходимости создания на АРМ пользователя дополнительных электронных документов, содержащих защищаемую информацию, пользователь создает и хранит такие документы в строго отведенном для этого месте.

6. Печать документов, содержащих защищаемую информацию, осуществляется только при наличии производственной необходимости на принтер, подключенный Администратором к АРМ пользователя. Печать документов, содержащих защищаемую информации, на общий сетевой принтер возможна только в том случае, когда в локальной сети все АРМ входят в состав одной ИСПДн. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих защищаемую информацию, уничтожаются.

7. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИС пользователь обязан выключить компьютер либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих Администрации Пристенского района Курской области пользователь обязан закрыть дверь помещения на ключ или применить другой используемый ограничитель доступа.

8. Покидая рабочее помещение в конце рабочего дня, пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.

Приложение № 4
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
по контролю за обеспечением уровня защищенности информации, содержащейся в информационных системах Администрации Пристенского района Курской области

1. Общие положения

1.1. Настоящая инструкция определяет организацию и порядок проведения контроля за обеспечением установленного уровня защищенности информации в информационных системах (далее - ИС) Администрации Пристенского района Курской области, обрабатывающих защищаемую информацию, в т.ч. персональные данные.

1.2. Инструкция является документом, обязательным для выполнения всеми должностными лицами при проведении работ, требующих защиты информации.

2. Цели и задачи контроля состояния защиты информации

2.1. Контроль состояния защиты информации в информационных системах (контроль защищенности ИС) Администрации Пристенского района Курской области осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к информации, преднамеренных специальных воздействий на информацию (носители информации) и других угроз информационной безопасности.

2.2. Основными задачами контроля являются:

– проверка соответствия принятых и принимаемых мер по защите информации нормативно-правовым требованиям;

– проверка своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите информации в Администрации Пристенского района Курской области.

При проведении контроля необходимо обеспечить подтверждение того, что:

– созданная система безопасности обеспечивает выполнение требований по защите информации при эксплуатации ИС;

– меры, средства и мероприятия, проводимые в целях защиты информации, соответствуют предъявляемым к ИС требованиям безопасности информации;

– средства защиты информации настроены и используются правильно;

– рекомендации предшествующих проверок реализованы.

3. Организация контроля

3.1. Организация мероприятий по проведению контроля за обеспечением установленного уровня защищенности информации в ИС осуществляется лицом, ответственным за защиту информации и обеспечение защиты персональных данных при их обработке в ИС.

3.2. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за защиту информации и обеспечение защиты персональных данных разрабатывает План мероприятий по защите информации в ИС (далее – План мероприятий).

3.3. Контроль состояния защиты информации в ИС проводится экспертной комиссией, образованной по приказу руководителя Администрации Пристенского района Курской области, в состав которой могут входить:

– ответственный за организацию обработки персональных данных;

– ответственный за защиту информации и обеспечение защиты персональных данных;

– администратор безопасности информации;

– администратор информационной системы;

– пользователи информационной системы;

– иные компетентные лица.

3.4. Результатом работы комиссии является формирование отчетных материалов (актов, заключений) выполнения мероприятий в соответствии с Планом мероприятий, содержащие результаты контроля.

3.5. Члены экспертной комиссии, осуществляющей контроль, имеют право:

– знакомиться с организацией работ по защите информации в ИС;

– получать по запросу в печатном виде документацию, касающуюся функционирования ИС;

– получать доступ ко всем помещениям, шкафам, стеллажам, сейфам, где размещены технические средства ИС и хранятся носители информации;

– требовать демонстрации режимов функционирования системы, конфигурации аппаратных и программных средств, их настроек и других параметров, влияющих на безопасность ресурсов ИС;

– получать доступ к журналам регистрации событий, происходящих в ИС;

– получать информацию о нарушениях безопасности в ИС и результаты разбора этих нарушений при наличии таковых;

– знакомиться с работой пользователей ИС.

3.6. Пользовательский персонал ИС Администрации Пристенского района Курской области должен содействовать проверяющим в реализации вышеуказанных прав.

3.7. Представители органов, осуществляющих контроль (эксперты), обязаны выполнять правила и распорядок работы отделов Администрации Пристенского района Курской области, а также не должны препятствовать работе пользователей ИС.

3.8. Проверка работоспособности средств защиты в рамках контрольных мероприятий проводятся в соответствии с программами проведения контроля состояния защиты информации в ИС, которые разрабатываются членами комиссии или привлечёнными сторонними организациями.

3.9. В результатах контроля должны содержаться оценка состояния защиты информации в ИС и, при необходимости, рекомендации по устранению недостатков и/или по совершенствованию системы защиты информации в ИС.

3.10. Работы по контролю (оценки) состояния защищенности ИС могут проводиться собственными силами и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации и лицензию ФСБ на осуществление деятельности по криптографической защите информации.

3.11. Периодичность проведения контроля за обеспечением уровня защищенности информации, содержащейся в информационных системах, должна осуществляться с учетом особенностей функционирования информационных систем, но не реже 1 раза в два года.

4. Планирование мероприятий по защите информации

4.1. В рамках планирования мероприятий по защите информации в Администрации Пристенского района Курской области применительно к каждой ИС осуществляется разработка, согласование и утверждение ежегодного Плана мероприятий по защите информации в ИС.

4.2. По решению руководителя Администрации Пристенского района Курской области допускается разработка единого плана мероприятий на несколько ИС.

4.3. План мероприятий разрабатывается лицом, ответственным за планирование и контроль мероприятий по защите информации в ИС (далее - Ответственный), с участием пользователей, эксплуатирующих ИС, и ответственных, обеспечивающих функционирование ИС.

4.4. В план мероприятий должны быть включены мероприятия по защите информации сегментов ИС, функционирующих в Администрации Пристенского района Курской области.

4.5. План мероприятий должен включать комплекс организационных и технических мероприятий по защите информации,

направленных на решение задач обеспечения информационной безопасности ИС.

4.6. Разработка мероприятий по защите информации должна осуществляться в соответствии с требованиями нормативных правовых актов в области защиты информации и принятыми в ОИВ локальными актами по защите информации.

4.7. План мероприятий включает следующие сведения по каждому из мероприятий:

- наименование мероприятий по защите информации;
- категория контрольных мероприятий;
- объекты контроля;
- процедуры/инструменты, применяемые для выполнения мероприятия;
- основания для проведения мероприятий;
- сроки и этапы проведения контрольных мероприятий;
- состав участников, привлекаемых для проведения контрольных мероприятий;
- наименования отделов (сотрудников), ответственных за реализацию каждого мероприятия.

4.8. План мероприятий должен содержать перечень мероприятий по защите конфиденциальной информации в ИС в хронологическом порядке.

4.9. План мероприятий формируется в следующем порядке:

- в срок не позднее 1 октября каждого года Ответственный формирует проект плана мероприятий;
- сформированный проект плана мероприятий подлежит согласованию с руководителем Администрации Пристенского района Курской области, администратором безопасности информации ИС, ответственным за организацию обработки ПДн, пользователями ИС и Комитетом в срок не позднее 1 ноября каждого года;
- согласованный проект плана мероприятий предоставляется Ответственным руководителю Администрации Пристенского района Курской области на утверждение.

Проект плана мероприятий подлежит рассмотрению и утверждению руководителем Администрации Пристенского района Курской области не позднее 30 декабря каждого года.

Утвержденный План мероприятий доводится Ответственным до работников Администрации Пристенского района Курской области в части, их касающейся.

4.10. Изменения в действующий план мероприятий вносятся в соответствии с разделом 5 настоящей Инструкции.

5. Порядок внесения изменений в план мероприятий

5.1. Внесение изменений в План мероприятий осуществляется на основании распоряжения руководителя Администрации Пристенского района Курской области, на основе предложений Ответственного.

5.2. Предложения о внесении изменений в План мероприятий могут быть сформированы в случаях:

- изменения законодательства Российской Федерации в области защиты информации;
- выявления в ходе контроля выполнения мероприятий, предусмотренных утвержденным Планом мероприятий, обстоятельств, требующих изменения Плана мероприятий (сроков, состава мероприятий, формулировок и т.д.);
- возникновения иных причин, препятствующих проведению мероприятия.

6. Проведение контроля

6.1. Контроль состояния защиты информации заключается в:

– проверке соблюдения требований правовых и организационно-распорядительных и нормативных документов по защите информации;

– проверке установленных характеристик информационной системы (состав подсистем, места установки, состав установленного программного обеспечения и технических средств)

– проверке функционирования, параметров настройки и работоспособности применяемых мер и средств защиты информации в соответствии с их эксплуатационной документацией и данными первичной проверки;

– анализе уязвимостей информационной системы и принятие мер защиты информации по их устранению;

– анализе изменения угроз безопасности информации в информационной системе;

– проверке знаний и выполнения пользователями своих функциональных обязанностей в части защиты информации;

– документировании процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе.

6.2. При проведении работ по контролю состояния защиты ИС должна быть проведена оценка и контроль реализации мер защиты в подсистемах:

– идентификации и аутентификации субъектов доступа и объектов доступа;
– управления доступом субъектов доступа к объектам доступа;
– ограничения программной среды;
– защиты машинных носителей информации;
– регистрации событий безопасности;
– антивирусной защиты;
– контроля (анализа) защищенности информации;
– обеспечения целостности информационной системы и информации;
– защиты технических средств;

– защиты информационной системы, ее средств, систем связи и передачи данных

– криптографической защиты информации.

6.3. По результатам проведения контрольных мероприятий на основании сформированных отчетных материалов принимается решение, о необходимости доработки (модернизации) системы защиты информации в ИС.

6.4. Каждое мероприятие Плана мероприятий должно быть реализовано в установленные сроки. Контроль за выполнением мероприятий, предусмотренных Планом мероприятий, осуществляется Ответственным.

6.5. Ответственный, руководствуясь сроками выполнения мероприятий, осуществляет проверку выполнения мероприятий ответственными лицами, основываясь на документальном подтверждении факта выполнения мероприятий.

6.6. В случаях выявления фактов неисполнения мероприятий (в том числе неполного исполнения), предусмотренных Планом мероприятий, Ответственный при взаимодействии с лицами, ответственными за выполнение мероприятий, проводит:

- установление причин неисполнения мероприятий (в срок не более 5 рабочих дней с момента выявления факта неисполнения мероприятия);

- подготовку предложений по корректировке Плана мероприятий (в срок не более 10 рабочих дней с момента установления причин неисполнения мероприятия).

6.7. С целью оценки эффективности обеспечения безопасности информации Ответственный ежегодно готовит отчет о выполнении Плана мероприятий, который представляется руководителю Администрации Пристенского района Курской области.

7. Ответственность лица, ответственного за планирование и контроль мероприятий по защите информации в информационных системах

Ответственный несет персональную ответственность за:

- качественную и своевременную подготовку Плана мероприятий;

- своевременный и качественный контроль за выполнением Плана мероприятий.

Приложение № 5
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Порядок выявления инцидентов информационной безопасности и реагирование на них

1. В качестве источников информации об инцидентах могут использоваться:

- журналы и оповещения системного и прикладного ПО ИС, обрабатывающих защищаемую информацию;
- журналы и оповещения СЗИ;
- оповещения средств обнаружения вторжений;
- информация, получаемая от работников ОИВ;
- информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

2. При обнаружении инцидента ответственный за выявление инцидентов информационной безопасности и реагирование на них должен оповестить ответственного за организацию обработки ПДн в ИС и руководителя Администрации Пристенского района Курской области.

3. Ответственный за управление инцидентами должен провести анализ инцидента информационной безопасности в целях выявления факта или предпосылки негативного воздействия на защищаемую информацию. В ходе анализа инцидента по возможности следует выявить следующие показатели:

- факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее - угроза);
- опасность угрозы;
- области, перечни информационных ресурсов, затрагиваемые воздействием угрозы;
- потенциальные нарушители, цели и причины реализации угрозы;
- перечень мер по локализации и остановке распространения действия угрозы.

4. Ответственный за управление инцидентами оповещает ответственного за организацию обработки ПДн о ходе и результатах реагирования на инциденты.

5. Ответственный за управление инцидентами вносит предложения ответственному за организацию обработки ПДн о недопущении повторных инцидентов. При необходимости ответственный за организацию обработки ПДн обеспечивает реализацию данных предложений.

Приложение № 6
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
по обеспечению антивирусной защиты в информационных системах Администрации Пристенского района Курской области

1. Общие положения

1.1.Настоящая Инструкция определяет порядок обеспечения антивирусной защиты информации, обрабатываемой в информационных системах Администрации Пристенского района Курской области.

1.2.Настоящая Инструкция предназначена для администратора безопасности информации (далее - Администратор).

1.3.В настоящей Инструкции используются следующие сокращения:

- АРМ — авторизированное рабочее место;
- НСД — несанкционированный доступ;
- ПО — программное обеспечение;
- САЗ — средство антивирусной защиты;
- СЗИ — средство защиты информации.

1.4.В настоящей Инструкции используются следующие термины и их определения:

– Антивирусная защита (информации) — организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий вредоносного ПО на информацию и (или) устранение последствий этих действий;

– Антивирусные базы — список сигнатур и алгоритмов, используемые средством антивирусной защиты для идентификации и (или) противодействия вредоносному ПО;

– Вирус (компьютерный, программный) — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению;

– Вредоносное ПО — программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на ресурсы АС[1];

[1] В настоящей Инструкции, понятие «вредоносное ПО» используется для определения совокупности вирусов, троянских коней, червей, руткитов и др.

– Зараженный ресурс — ресурс, подвергшийся программному воздействию;

– Лечение зараженных ресурсов — осуществляемые с использованием САЗ действия по восстановлению оригинального (до программного воздействия) содержимого зараженных ресурсов;

– Монитор (модуль САЗ) — модуль САЗ, постоянно находящийся в оперативной памяти и отслеживающий подозрительные действия других программ в режиме реального времени;

– Программное (программно-математическое) воздействие — несанкционированное воздействие на ресурсы информационной системы, осуществляемое с использованием вредоносного ПО;

– Ресурсы (информационные) — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах[2];

– Сканер (модуль САЗ) — модуль САЗ, предназначенный для проверки наличия вредоносного ПО в файлах, папках и дисках по требованию субъектов доступа;

– Средство антивирусной защиты (информации) — программное или программно-аппаратное средство, обеспечивающее антивирусную защиту информации.

1.5.Администратор безопасности информации, нарушивший требования настоящей Инструкции, несет персональную ответственность в соответствии с законодательством РФ.

1.6 Все администраторы безопасности должны быть под подпись ознакомлены с данной Инструкцией, а также ответственностью за нарушение ее требований.

2. Проведение антивирусного контроля на ПЭВМ

2.1. В целях обеспечения антивирусной защиты в информационных системах вводится антивирусный контроль.

2.2. К применению в информационных системах допускается лицензионное антивирусное программное обеспечение, имеющее действующие сертификаты ФСТЭК и/или ФСБ России.

2.3. Администратор осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

2.4. Администратор проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

2.5. При обнаружении компьютерного вируса пользователь обязан немедленно поставить в известность Администратора и прекратить какие-либо действия на ПЭВМ.

---

[2] В качестве ресурсов в информационной системе могут выступать файлы, области памяти машинных носителей и др.

2.6. Администратор проводит в случае необходимости лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

2.7. В случае обнаружения на съемных носителях информации нового вируса, не поддающегося лечению, Администратор обязан запретить использование съемных носителей.

2.8. В случае обнаружения на жестком диске ПЭВМ вируса, не поддающегося лечению, Администратор обязан поставить в известность ответственного за организацию обработки персональных данных, запретить работу в информационной системе и в кротчайшие сроки, обновить пакет антивирусной программы. Если обновление антивирусных баз не дало результатов, запретить работу до устранения угрозы со стороны вредоносного ПО или принятия решения о дальнейшей работе ответственным за организацию обработки персональных данных.

3. Действия в случае обнаружения вредоносного ПО

3.1. При обнаружении САЗ вредоносного ПО (пользователем информационной системы, или самим администратором), должен провести мероприятия по уничтожению вредоносного ПО и лечению зараженных ресурсов АС с использованием САЗ.

3.2. Если процедура уничтожения вредоносного ПО и лечения зараженных ресурсов информационной системы завершилась успешно, администратор должен провести проверку всей информации на всех носителях, которые могли быть заражены.

3.3. При невозможности уничтожения вредоносного ПО и (или) лечения зараженных файлов на носителе информации, администратор должен запретить использование данного носителя (приостановить работу рабочей станции) и сообщить об этом лицу, ответственному за организацию обработки персональных данных для выработки решения о дальнейших действиях.

Приложение № 7
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
о действиях лиц, допущенных к работе в информационных системах Администрации Пристенского района Курской области, в случае возникновения нештатных ситуаций

1. Общие положения

1.1. Настоящая инструкция определяет действия лиц, допущенных к работе в информационных системах Администрации Пристенского района Курской области (далее - Администрация), в случае возникновения инцидентов в процессах обработки информации, в т.ч. персональных данных.

1.2. Положения настоящей инструкции обязательны для исполнения всеми должностными лицами, допущенными к работе в информационных системах, обрабатывающих защищаемую информацию в части выполнения возложенных на них обязанностей.

1.3. Общими требованиями ко всем лицам, допущенным к работе в информационных системах, в случае возникновения нештатной ситуации или другого инцидента являются:

– лицо, обнаружившее нештатную ситуацию или другой инцидент, немедленно ставит в известность администратора (сетевого или безопасности) информационной системы;

– администратор (сетевой или безопасности) обязан провести анализ ситуации и, в случае невозможности исправить положение, поставить в известность руководство Администрации. Кроме этого, администратор информационной системы для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей информационной системы;

– по факту возникновения инцидента и выяснению причин его проявления по решению руководства может быть назначена комиссия по реагированию на инциденты ИБ и проведено служебное расследование.

2. Действия пользователей информационной системы при возникновении нештатных ситуаций

2.1. Сбой программного обеспечения, включая программное обеспечение средств защиты информации.

2.1.1. Администратор информационной системы выясняет причину сбоя программного обеспечения (в т.ч. средств защиты информации). Если

привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор информационной системы сообщает руководителю Администрации для принятия решения, по существу.

2.2. Отключение электропитания технических средств информационной системы.

2.2.1. Администратор информационной системы проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения (в т.ч. средств защиты информации), а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор информационной системы сообщает руководителю Администрации для принятия решения, по существу.

2.3. Выход из строя технических средств информационной системы (рабочих станций, источников бесперебойного питания, программно-аппаратных средств межсетевого экранирования и т.д.).

2.3.1. Администратор информационной системы совместно с администратором безопасности информационной системы выполняют мероприятия по ремонту неисправного технического средства информационной системы.

2.3.2. В случае необходимости уведомить о выходе из строя технических средств информационной системы администратора информационной системы.

2.3.3. При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий с составлением акта. О произошедшем инциденте необходимо сообщить администратору безопасности для принятия решения, по существу.

2.4. Обнаружение вредоносной программы в программной среде средств автоматизации информационной системы.

2.4.1. При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженную рабочая станцию рекомендуется физически отсоединить от локальной вычислительной сети, и администратор безопасности информационной системы проводит анализ состояния рабочей станции.

2.4.2. После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

2.4.3. По факту появления ВП в локальной вычислительной сети

может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем.

2.5. Утечка информации.

2.5.1. При обнаружении утечки информации ставится в известность администратор безопасности информационной системы. По факту может быть произведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов информационной системы и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.6. Взлом операционной системы средств автоматизации информационной системы (несанкционированное получение доступа к ресурсам операционной системы).

2.6.1. При обнаружении взлома рабочей станции ставятся в известность администратор информационной системы и администратор безопасности информационной системы.

2.6.2. По возможности производится временное отключение рабочей станции от локальной вычислительной сети информационной системы для проверки на наличие ВП.

2.6.3. Администратором безопасности информационной системы проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

2.6.4. В случае необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

2.6.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в информационную систему, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах информационной системы.

2.7. Попытка несанкционированного доступа (НСД).

2.7.1. При попытке НСД администратором безопасности информационной системы проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.7.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, администратором информационной системы устанавливаются такие обновления.

2.7.3. По факту попытки НСД может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Администрации.

2.7.4. В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к информационной системе субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.8. Компрометация ключевой информации (паролей доступа).

2.8.1. При компрометации ключевой информации (пароля доступа) администратором безопасности информационной системы принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

2.8.2. О произошедшем инциденте сообщается руководителю Администрации для принятия решения, по существу.

2.9. Физическое повреждение или хищение оборудования технических средств информационной системы.

2.9.1. Сотрудником, обнаружившим физическое повреждение элементов информационной системы, ставятся в известность: администратор информационной системы, администратор безопасности информационной системы.

2.9.2. Администратором безопасности информационной системы проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов информационной системы и возможные угрозы информационной безопасности.

2.9.3. О факте повреждения элементов информационной системы в случае необходимости администратор безопасности информационной системы докладывает руководителю Администрации.

2.9.4. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

2.9.5. Администратором безопасности информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.9.6. При необходимости администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения из эталонных копий с составлением акта.

2.10. Невыполнение установленных правил ИБ (правил работы информационной системы), использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.10.1. Сотрудником, обнаружившим невыполнение установленных правил ИБ, использование информационной системы с нарушением требований, установленных в нормативно-технической и (или)

конструкторской документации, ставятся в известность администратор безопасности информационной системы.

2.10.2. Администратором безопасности информационной системы проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.10.3. Об обнаруженном факте администратор безопасности информационной системы в случае необходимости докладывает руководителю Администрации.

2.10.4. При необходимости по решению руководителя Администрации по фактам выявленных нарушений проводится служебное расследование.

2.11. Ошибки сотрудников.

2.11.1. В случае возникновения сбоя, связанного с ошибками сотрудников, администратором безопасности информационной системы проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения.

2.11.2. При необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий с составлением акта.

2.11.3. В случае нанесения значительного ущерба вследствие ошибок работников по решению руководства Администрации может быть проведено служебное расследование.

2.12. Отказ в обслуживании.

2.12.1. Сотрудником, обнаружившим отказ в обслуживании, ставятся в известность администратор безопасности информационной системы.

2.12.2. Администратором безопасности информационной системы проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.12.3. Администратором безопасности информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.12.4. При необходимости, проводятся мероприятия по восстановлению программного обеспечения с составлением акта.

2.12.5. О причинах инцидента и принятых мерах администратор безопасности информационной системы в случае необходимости информирует руководителя Администрации.

2.13. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) информационной системы.

2.13.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) информационной системы администратором безопасности информационной системы проводится анализ с целью оценки возможности

утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.13.2. Администратором информационной системы совместно с администратором безопасности информационной системы проводятся мероприятия по восстановлению программного обеспечения, а также (при необходимости) проверка на наличие компьютерных ВП.

2.13.3. Об инциденте необходимо доложить руководителю Администрации.

2.14. Техногенные и природные проявления нештатных ситуаций.

2.14.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику, обнаружившему факт возникновения нештатной ситуации:

– немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения;

– немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);

– немедленно сообщить своему администратору АП и администратору безопасности.

2.14.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.14.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

3. Меры по обеспечению возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

3.1. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

– восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

– восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

– возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, позволяющих решать задачи по обработке информации.

Приложение № 8
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
по организации резервного копирования в информационных системах Администрации Пристенского района Курской области

1. Общие положения

Настоящая инструкция определяет действия, связанные с функционированием в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию, меры и средства поддержания непрерывности работы и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах.

Целью настоящего документа является превентивная защита элементов информационной системы от предотвращения потери защищаемой информации.

Задачей данной инструкции является:

– определение мер защиты от потери информации;

– определение действий восстановления в случае потери информации.

Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам информационной системы, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности информационной системы.

2. Порядок организации резервного копирования в информационной системе

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационной системы в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемой информации – не реже раза в неделю;

– для технологической информации – не реже раза в месяц;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы информационной системы – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Резервному копированию подлежит информация следующих основных категорий:

– персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;

– информация, обрабатываемая пользователями в информационной системе, а также информация, необходимая для восстановления работоспособности информационной системы, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;

– рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения информационной системы;

– регистрационная информация системы информационной безопасности информационной системы;

– другая информация информационной системы, по мнению пользователей и администраторов, являющаяся критичной для работоспособности информационной системы.

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Машинные носители информации, на которые произведено резервное копирование, должны быть учтены в журнале учета машинных носителей для архивного копирования информации, который находится у администратора безопасности. В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

Физический доступ к архивным копиям предоставляется только администратору информационной системы и администратору безопасности.

Передача машинных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

В случае необходимости восстановление данных из резервных копий производится администратором информационной системы или администратором безопасности.

Восстановление данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

3. Ответственность

Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности информационной системы.

Приложение № 9
к Инструкции по защите
конфиденциальной информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
по защите информации о событиях безопасности в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию

1. Общие положения

Настоящая инструкция по организации защиты информации о событиях безопасности в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию, определяет основные мероприятия по защите информации о событиях безопасности в информационных системах.

2. Основные мероприятия по защите информации о событиях безопасности

События безопасности, подлежащие регистрации в информационной системе, определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации в информационных системах, отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также нарушения штатного функционирования средств защиты информации.

В информационных системах определены следующие события безопасности, подлежащие регистрации:

1. События, связанные с регистрацией входа (выхода) субъектов доступа в систему и загрузки операционной системы. Состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2. События, связанные с регистрацией подключения машинных носителей информации и вывода информации на носители информации. Состав и содержание регистрационных записей включает: дату и время

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

3. События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4. События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

5. События, связанные с регистрацией попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей). Состав и содержание информации должны включать: дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер)).

6. События, связанные с изменением привилегий учетных записей.

7. События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления.

8. События, связанные с регистрацией запланированного обновления ОС (ведется в штатных журналах ОС). Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации, и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе.

Так же подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется администратором безопасности, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору безопасности информационной системы.

В информационной системе для обеспечения защиты информации о событиях безопасности, перед установкой СЗИ осуществляется синхронизация системного времени и даты. Администратор безопасности осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы и установленных СЗИ.

В информационной системе должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

Реагирование на сбои при регистрации событий безопасности должно предусматривать:

– предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
– реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

В целях предотвращения сбоев при регистрации событий безопасности СЗИ и операционной системы в информационной системе:

1. Администратору безопасности необходимо еженедельно проверять журналы регистрации событий СЗИ и операционной системы на наполненность и, в случае необходимости, производить их архивацию.

2. Увеличить при необходимости объем выделяемой под журналы событий безопасности СЗИ и операционной системы памяти.

3. Включить автоматическую перезапись новых событий безопасности поверх устаревших для предотвращения возникновения ошибок переполнения журналов.

4. Настройки прав учетных записей пользователей информационной системы должны исключать возможность внесения пользователями изменений в журналы событий безопасности, настройки СЗИ и операционной системы.

5. При появлении в информационных системах ошибок операционной системы или СЗИ пользователю необходимо уведомить администратора безопасности и приостановить работу до устранения ошибки.

Приложение № 10
к Инструкции по защите
конфиденциальной
информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
о порядке изменения состава и конфигурации технических и программных средств в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию

1. Общие положения

Настоящей инструкцией регламентируется порядок проведения модификации программного обеспечения и технического обслуживания средств вычислительной техники в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию.

Право внесения изменений в конфигурацию программно-аппаратных средств информационных узлов (рабочих станций, серверов) и телекоммуникационного оборудования, предназначенного для обработки информации в информационной системе, предоставляется:

– в отношении системных и прикладных программных средств, а также в отношении аппаратных средств информационной системы и программно-аппаратных средств телекоммуникаций – администратору информационной системы;

– в отношении программно-аппаратных и программных СЗИ - администратору безопасности.

Изменение конфигурации аппаратно-программных средств защищенных рабочих станций (АРМ) и серверов кем-либо, кроме перечисленных лиц, запрещено.

2. Порядок внесения изменений в конфигурацию программных и аппаратных средств информационной системы

Для внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций информационной системы начальнику структурного подразделения, в котором вносятся изменения, подается заявка на имя администратора безопасности, которая им рассматривается.

В заявках могут быть указаны следующие виды необходимых изменений в составе программных и аппаратных средств рабочих станций и серверов подразделения:

– установка в подразделении новой рабочей станции (АРМ) или сервера;

– замена рабочей станции (АРМ) или сервера подразделения;

– изъятие рабочей станции (АРМ) или сервера подразделения;

– добавление устройства (узла, блока) в состав конкретной рабочей станции (АРМ) или сервера подразделения;

– замена устройства (узла, блока) в составе конкретной рабочей станции (АРМ) или сервера подразделения;

– изъятие устройства (узла, блока) из состава конкретной рабочей станции (АРМ) или сервера;

– установка (развертывание) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной рабочей станции или сервере);

– обновление (замена) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

– удаление с конкретной рабочей станции (АРМ) или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

В заявке указываются условные наименования развернутых рабочих станций (АРМ) и серверов в соответствии с их паспортами. Программные средства указываются в соответствии с перечнем программных средств и программ, которые используются в информационной системе.

Администратор безопасности при согласовании заявки учитывает возможность совмещения решения новых задач (обработки информации) на указанных в заявке рабочих станциях (АРМ) или серверах в соответствии с требованиями по безопасности.

Все изменения в конфигурации технических и программных средств информационной системы должны производиться только после их согласования с органом по аттестации, выдавшим «Аттестат соответствия» на информационную систему.

После этого осуществляется непосредственное исполнение работ по внесению изменений в конфигурацию рабочих станций (АРМ) или серверов информационной системы.

Начальник структурного подразделения, в котором установлены аппаратно-программные средства, подлежащие модернизации, допускает уполномоченных исполнителей (администратора информационной системы и (или) администратора безопасности) к внесению изменений в состав аппаратных средств и ПО.

Установка, изменение (обновление) и удаление системных и прикладных программных средств производится администратором информационной системы.

Установка, снятие и внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов на рабочих станциях осуществляется администратором безопасности. Работы производятся в присутствии пользователя данной рабочей станции.

Установка или обновление подсистем информационной системы проводится в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Модификация ПО на сервере осуществляется администратором информационной системы по согласованию с администратором безопасности.

После установки модифицированных модулей на сервер администратор безопасности устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм с помощью специальных программных средств, прошедших оценку соответствия).

После проведения модификации ПО на рабочих станциях администратором безопасности должен быть проведен антивирусный контроль.

Установка и обновление общесистемного и прикладного ПО на рабочие станции (АРМ) и серверы производится с оригинальных лицензионных дистрибутивных носителей (компакт-дисков и др.), полученных установленным порядком.

Все добавляемые программные и аппаратные компоненты предварительно проверяются на работоспособность, контроль наличия проверок работоспособности осуществляет администратор информационной системы.

После установки (обновления) ПО, администратор информационной системы (при использовании специализированных СЗИ от НСД - администратор безопасности) производит настройку средств управления доступом к данному программному средству и проверяет работоспособность ПО и правильность настройки СЗИ.

После завершения работ по внесению изменений в состав аппаратных средств рабочей станции (АРМ), ее системный блок закрывается уполномоченным работником подразделения ИТ на ключ (при наличии штатных механических замков) и опечатывается (пломбируется, защищается специальной наклейкой) с возможностью постоянного визуального контроля за ее целостностью.

Уполномоченные исполнители работ производят соответствующую запись в журнале фактов вскрытия и опечатывания рабочих станций (серверов), выполнения профилактических работ, установки и модификации аппаратных и программных средств рабочих станций (серверов) информационной системы.

Администратор безопасности проводит периодический контроль за опечатыванием узлов и блоков информационной системы.

На обратной стороне заявки (Приложение 1) делается отметка о выполнении, и исполненная заявка передается администратору безопасности для хранения.

При изъятии рабочей станции (сервера) из состава информационной системы, ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как с данной рабочей станции (сервера) будут удалены все СЗИ и предприняты необходимые меры для затирания (удаления) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом об уничтожении информации, хранившейся на диске компьютера.

Приложение 1
к Инструкции о порядке
изменения состава и
конфигурации технических и
программных средств в
информационных системах
Администрации Пристенского
района Курской области,
содержащих защищаемую
информацию

(форма)

Администратору безопасности информации

ЗАЯВКА

на внесение изменений в состав аппаратно-программных/программных средств информационной системы

Прошу произвести следующие изменения конфигурации аппаратно-программных/программных средств информационной системы _____ в

(наименование информационной системы)

_____

(наименование подразделения)

развернуть новую рабочую станцию, установить на (обновить на / снять с) нее _____ компоненты, необходимые для решения следующих задач: _____

___

(наименование задач)

Начальник _____

(наименование подразделения)

«___» _____ 20__ г. _____ _____

(подпись) (фамилия и инициалы)

Отметка о выполнении:

_____ _____

(фамилия, инициалы) (подпись)

«_____» _____

Приложение № 11
к Инструкции по защите
конфиденциальной
информации
в информационных системах
Администрации
Пристенского района Курской
области

Инструкция
об использовании мобильных технических средств в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию

Настоящая инструкция определяет порядок использования мобильных технических средств в информационных системах Администрации Пристенского района Курской области, содержащих защищаемую информацию.

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

При использовании мобильных технических средств в информационных системах запрещается:

1. Обрабатывать защищаемую информацию на ноутбуках, используемых в качестве ОТСС за пределами контролируемой зоны;
2. Выносить за пределами контролируемой зоны ноутбуки, используемые в качестве ОТСС, кроме случаев передачи в ремонт;
3. Использовать мобильные технические средства информационной системы в целях, не связанных с обработкой защищаемой информацией в том числе ПДн;
4. Использовать в информационной системе съемные машинные носители информации, не зарегистрированные в журнале учета съемных носителей информации;
5. Подключение к элементам информационной системы, внешних устройств, не входящих в его состав (мобильных телефонов, цифровых фотоаппаратов, адаптеров беспроводной связи и иных).
6. Использовать в информационной системе беспроводные сети (WiFi, Bluetooth и др.);
7. Хранение на мобильных технических средствах информационной системы личной информации, а также информации, не имеющей отношения к служебной деятельности (музыкальные файлы, фоновые изображения и прочее).

Устройства ввода аудио (микрофоны) и видео (веб камеры) информации мобильных технических средств, используемых в информационной системе, должны быть отключены.

Администратором безопасности информационной системы обеспечивается:

Запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

Запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);

Очистка машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами контролируемой зоны;

Предоставление доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

Запрет использования устройств ввода аудио (микрофоны) и видео (веб-камеры) информации технических средств;

Подключение мобильных технических средств к ресурсам информационной системы должно осуществляться только по проводным каналам связи. Использование для подключения к ресурсам информационной системы беспроводных точек доступа (Wi-Fi и др.) запрещено.

Администратором безопасности информационной системы обеспечивается запрет подключения к беспроводным сетям доступа технических средств, имеющих в своем составе модули беспроводного доступа (моноблоки, стационарные АРМ, принтера и другие технические средства).

Ответственность за правильную эксплуатацию мобильных и технических средств, имеющих в своем составе модули беспроводного доступа, несут пользователи информационной системы и Администратор безопасности информационной системы.

Контроль за соблюдением пользователями правил эксплуатации мобильных технических средств и технических средств, имеющих в своем составе модули беспроводного доступа возлагается на Администратора безопасности информационной системы.

Контроль за соблюдением пользователями правил эксплуатации мобильных технических средств возлагается на администратора безопасности информационной системы.