**Концепция информационной безопасности Администрации городского округа Мытищи, утверждена Постановлением администрации городского округа Мытищи от 29/11/2016 №4002 "Об утверждении Концепции  информационной безопасности Администрации городского округа Мытищи "**

***Об утверждении Концепции информационной безопасности Администрации городского округа Мытищи***

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» и руководствуясь ст.ст. 40,44 Устава муниципального образования «Городской округ Мытищи Московской области»,

ПОСТАНОВЛЯЮ:

1. Утвердить Концепцию информационной безопасности Администрации городского округа Мытищи (Прилагается).

2. Управлению по работе с муниципальными организациями, охране труда, прохождению муниципальной службы, кадровой политики и наград (Керова Н.П.) ознакомить сотрудников, имеющих доступ к персональным данным в соответствии с должностными обязанностями, с положениями Концепции под роспись.

3. Возложить техническую поддержку организационно-технических мероприятий по обеспечению информационной безопасности на подразделение информационных технологий и связи Муниципального учреждения «Мытищинский центр бухгалтерского и материально-технического обеспечения».

4. Настоящее постановление разместить на официальном сайте органов местного самоуправления городского округа Мытищи.

5. Контроль за исполнением настоящего постановления оставляю за собой.

*Глава городского округа Мытищи  В.С. Азаров*

**Концепция информационной безопасности администрации городского округа Мытищи**

**СОДЕРЖАНИЕ**

|  |  |  |
| --- | --- | --- |
|  | Термины и определения……………………..……………………..…..………….. | 3 |
|  | Перечень сокращений……………………………………………….…………….. | 7 |
|  | Введение……………………………………………………………….……………… | 8 |
| 1. | Общие положения………………………………………………………..….……… | 9 |
| 2. | Цели и задачи обеспечения информационной безопасности …….………. | 10 |
| 3. | Объекты информационной безопасности ……………………..………..…… | 11 |
| 4. | Основные угрозы информационной безопасности …………….………… | 11 |
| 5. | Основные направления деятельности по обеспечению информационной безопасности ……………………………….………..…………………………….. | 12 |
| 6. | Принципы формирования системы информационной безопасности …… | 13 |
| 7. | Структура подразделений, обеспечивающих информационную безопасность. | 14 |
| 8. | Модель взаимодействия участников информационной системы………... | 14 |
| 9. | Меры, методы и средства обеспечения безопасности информационных систем……………………………………….…….….…………………………….…. | 15 |
| 10. | Порядок организации работ при разработке и эксплуатации информационных систем и системы обеспечения информационной безопасности………………………………….………………………….……..……. | 17 |
| 11. | Порядок управления системой обеспечения информационной безопасности………………………………….………………………….….…….…. | 17 |
| 12. | Контроль состояния информационной безопасности………….…………... | 18 |

ТЕРМИНЫ и ОПРЕДЕЛЕНИЯ

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**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.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей Администрации и посторонних транспортных, технических и иных материальных средств.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Побочные электромагнитные излучения и наводки** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

**Программная закладка** - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость ИСПДн** – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

**Целостность информации** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АВПО – антивирусной программное обеспечение

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

ИВС – информационная вычислительная система

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки

САЗ - система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Концепция информационной безопасности (далее - Концепция) администрации городского округа Мытищи (далее - Администрация) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Также в Концепции излагаются основные положения государственной политики обеспечения информационной безопасности Администрации, организационная структура и принципы построения информационной безопасности. Концепция служит методологической основой разработки комплекса правовых актов и организационно-методических документов, регламентирующих деятельность в области информационной безопасности Администрации.

Положения Концепции не распространяются на сведения, отнесенные к государственной тайне.

**1. Общие положения**

Целью настоящей Концепции является обеспечение безопасности объектов защиты Администрации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба при обработке информации вообще, и персональных данных в частности.

Концепция представляет собой принятую систему взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере и служит методологической основой изложенных направлений обеспечения информационной безопасности Администрации:

- разработка стратегии обеспечения информационной безопасности Администрации, включающей в себя цели, задачи и комплекс основных мер по ее практической реализации, формирования и проведения государственной политики Администрации в области обеспечения информационной безопасности;

- обеспечение единого понимания всеми участниками процесса информатизации в Администрации проблем информационной безопасности;

- определение уровней информационной безопасности объектов информатизации Администрации;

- разработка единых подходов к построению программно-технических систем защиты объектов информатизации Администрации;

- обеспечение условий гармонизации информационной инфраструктуры Администрации с глобальными информационными сетями и системами.

Комплексная система информационной безопасности Администрации должна обеспечивать безопасное использование информационных ресурсов Администрации и получение информационных услуг.

Концепция служит методологической основой:

- формирования и проведения единой политики Администрации в области обеспечения информационной безопасности;

- разработки целевых программ Администрации по обеспечению защиты информационных систем и ресурсов телекоммуникаций;

- разработки и внедрения технологий информационной безопасности Администрации;

- подготовки предложений по совершенствованию правового, организационного, технического и программного обеспечения информационной безопасности Администрации.

Положения Концепции должны учитываться при создании информационных ресурсов и систем, развитии информационных технологий, создании и развитии единого информационного пространства Администрации.

Правовую основу Концепции составляют Конституция Российской Федерации, Указ Президента Российской Федерации от 12 мая 2009 года № 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года", Указ Президента Российской Федерации от 17 марта 2008 года № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Доктрина информационной безопасности Российской Федерации, утвержденная приказом Президента Российской Федерации от 09 сентября 2000 года № Пр-1895, Федеральный закон от 28 декабря 2010 года № 390-ФЗ "О безопасности", Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных", Федеральный закон от 10 января 2002 года № 1-ФЗ "Об электронной цифровой подписи", Федеральный закон от 06 апреля 2011 года № 63-ФЗ "Об электронной подписи" и иные правовые акты.

**2. Цели и задачи обеспечения информационной безопасности**

Целью построения системы информационной безопасности Администрации является защита объектов информационной безопасности от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий персонала или иных форм незаконного вмешательства в информационные ресурсы и информационные системы.

Основные задачи обеспечения информационной безопасности Администрации:

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся и обрабатываемых в информационных системах;

- обеспечение соблюдения требований законодательства Российской Федерации в области информационной безопасности;

- формирование и проведение единой политики в обеспечении информационной безопасности;

- организация и координация работ по информационной безопасности в различных сферах деятельности;

- возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого участника в пределах его полномочий;

- пересмотр и улучшение применяемых защитных мер, требований, норм и правил информационной безопасности с учетом изменения информационной среды и условий;

- осознание необходимости обеспечения информационной безопасности как неотъемлемой части культуры;

- постоянный контроль выполнения требований правовых актов, регламентирующих деятельность в области информационной безопасности;

- создание системы непрерывного обучения, тренировки и проверки осведомленности персонала по вопросам обеспечения информационной безопасности;

- осуществление деятельности по обеспечению доверия к информационной безопасности;

- обеспечение защиты информации от несанкционированного доступа на этапах сбора, обработки, хранения и предоставления конечному потребителю информации;

- предотвращение утраты, искажения или уничтожения информации на этапах сбора, обработки, хранения и предоставления конечному потребителю информации;

- обеспечение непрерывного функционирования информационных систем и системы обеспечения информационной безопасности;

- своевременное прогнозирование, выявление и нейтрализация угроз информационной безопасности;

- обеспечение эффективной работы механизмов оперативного реагирования на угрозы информационной безопасности;

- мониторинг состояния защищенности информации.

Достижение намеченной цели зависит от качественного решения основных задач в вопросе обеспечения информационной безопасности Администрации.

**3. Объекты информационной безопасности**

К объектам информационной безопасности Администрации относятся:

1) информационные ресурсы Администрации, содержащие конфиденциальную информацию (служебная тайна, коммерческая тайна, персональные данные и прочая информация), информацию ограниченного доступа, а также общедоступную информацию;

2) системы формирования, распространения и использования информационных ресурсов, включающие в себя информационные системы различного класса и назначения, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

3) информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования Администрации.

**4. Основные угрозы информационной безопасности**

Угроза информационной безопасности - совокупность факторов и условий, создающих опасность для нормального функционирования информационной инфраструктуры.

Источники угроз информационной безопасности Администрации разделяются на внешние и внутренние.

К внешним угрозам относятся:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных систем;

- перехват и утечка информации по техническим каналам;

- неконтролируемое самопроизвольное распространение компьютерных вирусов и иных вредоносных программ;

- стихийные бедствия, катастрофы, пожары и аварии.

Внутренними источниками угроз являются:

- невыполнение требований законодательства и несвоевременное принятие необходимых правовых актов, регламентирующих деятельность в сфере информационной безопасности;

- нарушения установленных регламентов сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, создающие предпосылки к утечке либо разглашению сведений, составляющих государственную, служебную и иную тайну;

- внедрение несовершенных или устаревших информационных технологий и средств информатизации;

- умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала;

- отказы, сбои, неисправности, несогласованности инженерно-технических, программных и системно-прикладных средств защиты информационных и телекоммуникационных систем;

- использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты и контроля информации;

- привлечение к работам по созданию, развитию и защите информационных систем сторонних организаций, не имеющих прав на осуществление соответствующих видов деятельности.

Приведенная выше классификация угроз носит условный характер, не является окончательной и не ранжирована по степени приоритетности. В объективной реальности угрозы, как правило, носят комбинированный характер.

Непрерывный процесс прогнозирования, выявления, идентификации, конкретизации, анализа и выработки мер по локализации угроз является неотъемлемой задачей текущей деятельности в построении системы информационной безопасности Администрации.

**5. Основные направления деятельности по обеспечению информационной безопасности**

Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

Основные направления обеспечения информационной безопасности:

1) правовое обеспечение информационной безопасности - деятельность в этой области направлена на создание и поддержание в актуальном состоянии системы локальных актов, регламентирующих деятельность по обеспечению информационной безопасности;

2) организация деятельности по обеспечению информационной безопасности - деятельность в этой области направлена на создание документированных процессов обеспечения информационной безопасности, скоординированных между структурными подразделениями Администрации;

3) обеспечение информационной безопасности при управлении информационными ресурсами - деятельность в этой области направлена на идентификацию, классификацию информационных ресурсов и их владельцев, формирование и поддержание необходимого уровня информационной безопасности информационных ресурсов;

4) обеспечение информационной безопасности, связанное с персоналом, - деятельность в этой области направлена на минимизацию рисков, вызванных действиями работников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех работников по вопросам обеспечения информационной безопасности;

5) физическая безопасность информационных ресурсов - деятельность в этой области направлена на минимизацию и предотвращение ущерба, вызванного физическим воздействием на информационные ресурсы;

6) обеспечение информационной безопасности на этапах жизненного цикла информации в информационной инфраструктуре - деятельность в этой области направлена на минимизацию рисков, возникающих в процессе создания, обработки, обмена и уничтожения информации в информационной инфраструктуре;

7) управление доступом к информационным ресурсам - деятельность в этой области направлена на создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа;

8) управление инцидентами информационной безопасности - деятельность в этой области направлена на создание процесса по своевременному выявлению и реагированию на инциденты информационной безопасности;

9) соответствие требованиям - деятельность в этой области направлена на соответствие требованиям законодательства, локальных нормативных актов по обеспечению информационной безопасности.

**6. Принципы формирования системы информационной безопасности**

Реализация основных концептуальных направлений информационной безопасности Администрации осуществляется на основе следующих принципов:

1) централизация управления - предполагает, что деятельность по обеспечению информационной безопасности должна быть встроена в управленческие процессы Администрации, подчиняться понятным руководителям закономерностям и оцениваться с позиций эффективности, для этого процессы обеспечения информационной безопасности должны быть организованы, управляемы и оцениваемы подобно другим процессам и согласованы с ними;

2) законность - предполагает осуществление защитных мероприятий и разработку системы информационной безопасности в соответствии с действующим законодательством в области информационных технологий и защиты информации;

3) персональная ответственность - предполагает персональную ответственность в пределах должностных полномочий за несоблюдение регламентирующих документов в области информационной безопасности;

4) минимизация полномочий - предполагает предоставление прав доступа сотрудникам Администрации к информационным ресурсам в объеме, достаточном для качественного выполнения своих должностных (функциональных) обязанностей;

5) своевременность - предполагает своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружение угроз, потенциально способных нанести ущерб;

6) системность - системный подход к построению системы информационной безопасности предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения информационной безопасности, включающим фазы планирования, реализации, контроля и совершенствования системы информационной безопасности;

7) комплексный подход - предполагает всестороннее обеспечение информационной безопасности и предусматривает использование взаимоувязанных программно-технических, организационных, правовых, нормативно-методических и других мер обеспечения информационной безопасности на единой концептуальной основе;

8) непрерывность - предполагает непрерывный, целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных мер защиты;

9) унифицированность - предполагает, что принципы, правила, процедуры, требования и технические решения по обеспечению информационной безопасности должны быть унифицированы;

10) простота - предполагает, что порядок действий и процесс использования средств защиты информации должны быть понятны пользователю.

**7.Структура подразделений, обеспечивающих информационную безопасность Администрации**

Основываясь на принципах построения системы информационной безопасности Администрации, определяется структурное подразделение, отвечающее за обеспечение информационной безопасности во всех структурных подразделениях, которое наделяется соответствующими полномочиями и обязанностями:

разработка правовых актов по информационной безопасности Администрации;

проведение проверочных мероприятий по информационной безопасности Администрации;

выбор средств обеспечения информационной безопасности информационных и телекоммуникационных систем Администрации;

создание и развитие системы защиты информации Администрации;

администрирование системы защиты информации Администрации;

участие в разработке (доработке) подсистем защиты информации в информационных системах Администрации.

Глава Администрации несет ответственность за организацию работ по обеспечению информационной безопасности.

**8. Модель взаимодействия участников информационной системы**

Моделирование информационной системы необходимо для описания процессов информационного взаимодействия в информационной системе и определения зон ответственности.

Участник информационной системы - физическое или юридическое лицо, непосредственно взаимодействующее с информационной системой.

Участники информационной системы подразделяются на 4 группы:

1) Владельцы информационной системы.

Зона ответственности:

- разработка (доработка) информационной системы;

- поддержание работоспособности информационной системы;

- защита информации в информационной системе;

- определение круга пользователей информации.

2) Оператор информационной системы.

Зона ответственности:

- эксплуатация информационной системы, обработка информации.

3) Поставщик (владелец) информации.

Зона ответственности:

- достоверность и своевременность предоставляемой информации;

- наделение пользователей информации правами на получение информации из информационной системы.

4) Пользователь информации.

Зона ответственности:

- соблюдение правил и прав на получение информации из информационной системы;

- сохранение конфиденциальности полученных из информационной системы сведений.

Участник информационной системы может одновременно находиться в нескольких группах.

Владелец информационной системы при разработке (доработке) информационной системы взаимодействует со структурным подразделением, отвечающим за обеспечение информационной безопасности Администрации, в том числе:

1) представляет документацию на информационную систему;

2) согласует документацию на разработку (доработку) информационной системы;

3) информирует о ходе проведения работ по обеспечению информационной безопасности информационной системы.

Оператор информационной системы взаимодействует с владельцем информационной системы и структурным подразделением, отвечающим за обеспечение информационной безопасности во всех структурных подразделениях Администрации, в том числе:

1) представляет документы, регламентирующие правила получения информации из информационной системы;

2) представляет документы, регламентирующие права пользователей на информацию;

3) представляет документы, регламентирующие правила приема информации в информационную систему.

**9. Меры, методы и средства обеспечения безопасности информационных систем**

Анализ технических, структурных, эксплуатационных и иных особенностей информационных систем имеет важное значение для организации и внедрения надежной системы обеспечения информационной безопасности.

При выборе и использовании комплекса методов, способов и средств защиты информации, необходимых для обеспечения безопасности информации в конкретных информационных системах, должны учитываться такие факторы, как:

- наличие конфиденциальной информации (персональные данные, служебная тайна и т.д.);

- условия размещения и эксплуатации технических средств;

- способы обработки данных в системе;

- особенности обработки и пересылки информации в электронном виде;

- количество пользователей и способы организации их работы с информационной системой;

- способы хранения информации.

Проблема обеспечения информационной безопасности может быть решена в результате комплексного применения всех мер защиты, включающих в себя:

- правовые (законодательные);

- организационные;

- технические.

**Правовые (законодательные) меры обеспечения безопасности информационных систем**

К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

Правовые (законодательные) меры обеспечения безопасности информационных систем выделяют правовую область, в пределах которой допускается использовать информационные ресурсы различных субъектов информационных отношений.

**Организационные меры обеспечения безопасности информационных систем**

Организационные меры обеспечения безопасности информационных систем - меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

**Технические меры обеспечения безопасности информационных систем**

Технические меры обеспечения безопасности информационных систем должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

При учете всех требований и принципов обеспечения безопасности информации в информационной системе в состав системы включают следующие технические и программные средства:

- идентификации пользователей;

- аутентификации пользователей (потребителей) информации и информационных объектов (терминалов, программных алгоритмов, элементов баз данных и т.п.), соответствующих степени конфиденциальности информации и обрабатываемых данных;

- разграничения доступа к данным;

- управления информационными потоками;

- информационной безопасности в линиях передачи данных, в хранилищах информации;

- обеспечения и контроля целостности программных и информационных ресурсов;

- регистрации и контроля обращений к информации, подлежащей защите;

- реагирования на попытки реализации несанкционированного доступа;

- активные и пассивные средства защиты информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.

**10. Порядок организации работ при разработке и эксплуатации информационных систем и системы обеспечения информационной безопасности**

Разработка любой прикладной информационной системы требует обязательной доработки системы обеспечения информационной безопасности, в связи с чем данные рабочие процессы должны протекать параллельно, без отрыва друг от друга.

Процессу разработки, модернизации информационной системы должен предшествовать процесс определения перечня информации, которую в будущем будут обрабатывать в данной системе, и присвоения категорий защищаемой информации.

Этапу ввода в эксплуатацию прикладной информационной системы должен предшествовать этап ввода в эксплуатацию разработанной (доработанной) системы информационной безопасности. Разработанная (доработанная) система информационной безопасности должна предусматривать:

- назначение уровня полномочий и должностных лиц, ответственных за присвоение категории обрабатываемой информации (служебная тайна, персональные данные, открытая информация общего пользования и т.д.);

- назначение уровня полномочий и должностных лиц, имеющих право распоряжаться информацией, - применительно к каждой категории защищаемой информации;

- условия и порядок допуска пользователей информации к работе с информацией - применительно к каждой категории защищаемой информации;

- определение объема информации, необходимой и достаточной для эффективного выполнения работниками организации своих прямых должностных обязанностей;

- определение границ применения информации пользователями информации;

- разработку необходимого пакета документов, регламентирующих работу в информационной системе.

Стадия ввода в действие прикладной информационной системы завершается аттестацией объекта информатизации, в состав которого вводится данная система.

**11. Порядок управления системой обеспечения информационной безопасности**

Управление системой обеспечения информационной безопасности Администрации представляет собой целенаправленное воздействие на ее компоненты, обеспечивающее защищенность информации, обрабатываемой в информационных системах.

Цель процесса управления системой обеспечения информационной безопасности - обеспечение надежной защиты информации в процессе ее сбора, обработки, хранения и предоставления (передачи) конечному пользователю информации.

Управление системой информационной безопасности Администрации должно осуществляться на всех этапах существования информационной системы, с момента проведения научно-технических изысканий, предшествующих проектным работам по созданию новой информационной системы до момента вывода этой системы из технической эксплуатации по причине ее морального устаревания.

Управление системой обеспечения информационной безопасности Администрации осуществляет структурное подразделение, отвечающее за информационную безопасность, объединяющие в своем составе квалифицированных специалистов в области информационных технологий и защиты информации.

**12. Контроль состояния информационной безопасности**

Контроль состояния информационной безопасности осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Основная решаемая задача - получение объективных оценок текущего состояния защиты информации ограниченного доступа, оценка эффективности применяемых мер и технических решений для обеспечения информационной безопасности Администрации, оказание методической помощи по обеспечению режима защиты информации, организация работы по обеспечению информационной безопасности.

Под постоянным контролем находятся:

- дисциплина выполнения правовых, организационно-распорядительных и нормативных документов Администрации;

- действующие меры обеспечения информационной безопасности;

- обоснованность и эффективность применения мер обеспечения информационной безопасности.

Общее состояние информационной безопасности контролирует 1-й заместитель главы Администрации, в компетенцию которого входит контроль за обеспечение информационной безопасности Администрации.

Техническую поддержку организационно-технических мероприятий по обеспечению информационной безопасности осуществляет подразделение информационных технологий и связи МУ «МЦБМТО».

С целью получения объективного заключения о состоянии информационной безопасности Администрации возможно привлечение специалистов уполномоченного исполнительного органа государственной власти Московской области, участвующего в поддержании и эксплуатации прикладных информационных систем, а также организации, обладающие соответствующими правами на осуществление деятельности в области защиты информации.

Оценка эффективности мер информационной безопасности проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.