Утвержден
приказом Нацстаткома КР
от 12 февраля 2024 года №13

Политика информационной безопасности
Национального Статистического комитета
Кыргызской Республики

Содержание

I. Общие положения

1. Назначение Политики информационной безопасности

Политика информационной безопасности (далее также “Политика”) Национального статистического комитета Кыргызской Республики (далее – НСК), определяет систему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач в области информационной безопасности, основных принципов построения системы безопасности информации в НСК.

Основные положения и требования Политики распространяются на все структурные подразделения НСК, включая подведомственные подразделения и территориальные органы НСК, всех сотрудников НСК (штатных, временных, работающих по контракту и т.п.), а также сторонних лиц, организаций и учреждений, осуществляющих взаимодействие с подведомственными подразделениями и территориальными органами НСК в качестве поставщиков и потребителей информационных ресурсов НСК.

2. Правовая основа Политики информационной безопасности

Правовой основой настоящей Политики являются Конституция Кыргызской Республики, Гражданский кодекс Кыргызской Республики, Уголовный кодекс Кыргызской Республики, Кодекс Кыргызской Республики о правонарушениях, законы Кыргызской Республики, Указы Президента Кыргызской Республики, постановления Кабинета Министров (Правительства) Кыргызской Республики, стратегические и программные документы Кыргызской Республики в сфере информационной безопасности, утвержденные Указом Президента Кыргызской Республики, постановлением Кабинета Министров Кыргызской Республики, другие нормативные правовые акты, регулирующие сферу информационной безопасности государственных органов Кыргызской Республики.

Политика разработана на основе анализа современного состояния и перспективы развития информационных технологий в НСК, анализа угроз информационной безопасности НСК и в соответствии с требованиями:

1) Законов Кыргызской Республики:

– «Об электронном управлении» от 19 июля 2017 года № 127;

– «О гарантиях и свободе доступа к информации» от 5 декабря 1997 года № 89;

– «О защите государственных секретов Кыргызской Республики» от 15 декабря 2017 года № 210;

– «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления Кыргызской Республики» от 28 декабря 2006 года № 213;

– «Об официальной статистике» от 8 июля 2019 года № 82;

– «Об информации персонального характера» от 14 апреля 2008 года

№ 58.

2) постановлений Правительства Кыргызской Республики;

– “Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем” от 21 ноября 2017 года № 762;

– «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года № 760;

– “О некоторых вопросах, связанных с государственными информационными системами” от 31 декабря 2019 года № 744.

Основные положения Политики направлены на:

1) формирование единой политики в области обеспечения информационной безопасности в НСК;

2) принятие управленческих решений и разработки практических мер по воплощению политики информационной безопасности и выработки согласованных мер, направленных на выявление, отражение и ликвидацию последствий различных видов угроз информационной безопасности;

3) координацию деятельности структурных подразделений и территориальных органов НСК при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению информационной безопасности;

4) разработки предложений по совершенствованию правового, технического и организационного обеспечения информационной безопасности в НСК.

3. Основные термины, сокращения и определения

Административные данные – информация, собираемая государственными органами и органами местного самоуправления с целью выполнения ими задач и функций, отнесенных к их компетенции в соответствии с законодательством Кыргызской Республики;

Атака на информационную систему – любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы;

Безопасность субъектов информационных отношений – защищенность жизненно важных интересов субъектов информационных отношений от нанесения им материального, морального или иного вреда путем воздействия на информацию и/или средства ее обработки и передачи;

Внутренний аудит информационной безопасности – объективный, документированный процесс контроля качественных и количественных характеристик текущего состояния информационной безопасности элементов государственной инфраструктуры электронного управления, осуществляемый самой организацией (владельцем/оператором информационной системы) в своих интересах;

Вредоносные программы – программы или измененные программы

объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы;

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими его идентифицировать;

Доступ к информации – ознакомление с информацией или получение возможности ее обработки, регламентируемый ее правовым режимом, определяющий строгое соблюдение его требований;

Доступ к ресурсу – получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом;

Доступность информации – важнейшее свойство системы, в которой циркулирует информация (средств и технологии се обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия;

Естественные угрозы – угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

Журналирование событий – процесс записи информации о происходящих программных или аппаратных событиях в электронный журнал регистрации событий;

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию;

Защита информации от несанкционированного доступа – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

Злоумышленник – нарушитель, действующий намеренно из корыстных, идейных или иных побуждений;

Идентификатор - последовательность символов, позволяющих однозначно идентифицировать статистическую единицу по ее имени/названию, точному географическому местоположению или идентификационному номеру;

Индивидуальные данные – детализированные данные о статистических единицах, применяемые при разработке, производстве и распространении официальной статистики;

Информация – сведения о предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

Информация персонального характера (персональные данные) - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать

этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности;

Информационная безопасность (кибербезопасность) – сохранение свойств целостности (которая может включать аутентичность и отказоустойчивость), доступности и конфиденциальности информации в объектах информационной инфраструктуры, обеспечиваемое за счет использования совокупности средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками и страхования, профессиональной подготовки, практического опыта и технологий;

Информационные ресурсы – отдельные документы и массивы документов в информационных системах;

Информационная среда – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений;

Информационная система НСК – организационно упорядоченная совокупность документов (массивов документов), независимо от формы их представления, и информационных технологий, в том числе с использованием вычислительной техники и связи;

Канал утечки информации – неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное (несанкционированное) овладение нарушителем защищаемой информацией;

Критически важное оборудование – оборудование, сбои в работе которого или отказ которого имеют существенное значение для выполнения НСК, его подведомственным подразделением или территориальным органом, осуществляющим полномочия владельца и/или оператора информационной системы своих основных функций, и приведут к невозможности выполнения (прекращению) возложенных на них функций;

Конфиденциальность информации – субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней;

Корпоративная информационная система – организационно-техническая система, представляющая собой совокупность взаимосвязанных компонентов: технических средств обработки и передачи данных, методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации;

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации;

Метаданные – данные и другая документация, которые описывают статистические данные и статистические процессы в стандартизованном виде путем предоставления информации об источниках данных, методах, определениях, классификациях и качестве данных;

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации;

Несанкционированный доступ – доступ субъекта к информации, объекту в нарушение требований ее правового режима, правил разграничения доступа;

НСК – Национальный статистический комитет Кыргызской Республики;

Объект – пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа;

Объект защиты – информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;

Организационные меры защиты – меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности, циркулирующей в ней информации;

Пароль – служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию;

Пользователь – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

Поставщики административных данных – государственные органы и органы местного самоуправления, предоставляющие производителям официальной статистики данные, собранные в административных целях;

Производство – все виды деятельности, связанные со сбором, обработкой, анализом и хранением данных в целях составления официальной статистики;

Разработка – деятельность по созданию, усилению и совершенствованию статистических методов, концепций, стандартов и процедур, используемых для производства и распространения официальной статистики;

Рабочая станция – стационарный или портативный компьютер в составе локальной сети, предназначенный для решения прикладных задач;

Разграничение доступа – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе;

Разграничение доступа к ресурсам – порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом

соответствии с установленными правилами;

Секретная информация – информация, циркулирующая в средствах вычислительной техники и связи, телекоммуникациях, а также другие информационные ресурсы, содержащие сведения, отнесенные к служебной и государственной тайне, представленные в виде информативных акустических и электрических сигналов, физических полей, материальных носителей информации, информационных массивов и баз данных;

Серверное помещение – помещение, предназначенное для размещения серверного, активного и пассивного сетевого (телекоммуникационного) оборудования и оборудования структурированных кабельных систем;

Система информационной безопасности – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности НСК;

Средство криптографической защиты информации – программное обеспечение или аппаратно-программный комплекс, реализующий алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами шифрования;

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации;

Субъект – активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа;

Субъекты информационных отношений – государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации;

Субъект персональных данных – физическое лицо, к которому относятся соответствующие персональные данные;

Технические (аппаратно-программные) средства защиты – различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.);

Техническая документация по кибербезопасности – документация, устанавливающая политику, правила, защитные меры, касающиеся процессов обеспечения целостности (включая аутентичность и отказоустойчивость), доступности и конфиденциальности информации, содержащейся в базах данных государственных информационных систем;

Угроза – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного

(неумышленного) нарушения режима функционирования объекта и нарушения свойств защищаемой информации или других ресурсов объекта;

Угроза безопасности информации – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

Уязвимость информации – подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию;

Физические меры защиты – это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации и другим ресурсам информационной системы, а также технические средства визуального наблюдения, связи и охранной сигнализации;

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

Цель защиты информации – предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты информационной системы, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

II. Основные принципы построения, цели и задачи системы информационной безопасности НСК

4. Основные принципы построения системы информационной безопасности НСК

Система Политики информационной безопасности строится с учетом основных принципов создания комплексных систем обеспечения информационной безопасности, характеристики и возможности организационно - технических методов и современных аппаратно - программных средств защиты и противодействия угрозам информационной безопасности.

Эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений.

Построение системы информационной безопасности НСК и ее функционирование должны осуществляться в соответствии со следующими

основными принципами:

1) ***принцип законности***, предполагающий:

– осуществление защитных мероприятий и разработку системы безопасности информации НСК в соответствии с действующим законодательством в области электронного управления, обеспечения информационной безопасности государственных информационных систем, а также других нормативных правовых актов по информационной безопасности;

– построение и управление системой информационной безопасности НСК в пределах собственной компетенции, с применением дозволенных методов обнаружения и пресечения правонарушений при работе с информацией;

2) ***принцип системности***, предполагающий системный подход к построению системы защиты информации в НСК с учетом взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности в НСК; при создании системы защиты должны учитываться все наиболее уязвимые места информационной системы НСК, а также характер, возможные объекты и направления угроз со стороны нарушителей (в особенности высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации;

3) ***принцип комплексности***, предполагающий комплексное использование методов и средств защиты информационных систем и построение целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

4) ***принцип непрерывности***, предполагающий деятельность по обеспечению информационной безопасности, осуществляемый постоянно на всех уровнях НСК, начиная от руководства НСК, подразделениями обеспечения информационной безопасности, подведомственными подразделениями и территориальными органами НСК, и продолжая участием в этом процессе каждого сотрудника НСК;

5) ***принцип своевременности***, предполагающий упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации;

6) ***принцип преемственности и непрерывности совершенствования***, предполагающий постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы НСК и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, передовых технологий и опыта в этой области;

7) ***принцип разумной достаточности*** *(экономической*

целесообразности), предполагающий соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения;

8) ***принцип персональной ответственности***, предполагающий возложение ответственности за обеспечение информационной безопасности и системы обработки информации на каждого сотрудника в пределах его полномочий;

9) ***принцип минимизация полномочий***, означающий предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью, только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей;

10) ***принцип статистической конфиденциальности,*** распространяющийся на следующие данные:

– агрегированные показатели, состоящие из одной-трех единиц, где единица представляет собой физическое, юридическое лицо или домохозяйство, если одна из этих единиц может быть косвенно идентифицирована; в исключительных случаях агрегированные показатели, состоящие из более трех единиц, могут быть объявлены председателем НСК конфиденциальными, если одна из этих единиц может быть косвенно идентифицирована;

– информацию, объявленную государственным секретом или банковской тайной в соответствии с законодательством в области защиты государственных секретов или банковской деятельности Кыргызской Республики;

11) ***принцип исключения конфликта интересов***, предполагающий четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов;

12) ***принцип взаимодействия и сотрудничества***, предполагающий создание благоприятной атмосферы в коллективах структурных подразделений НСК, в которой сотрудники понимают свою роль в процессе обеспечения информационной безопасности и принимают участие в этом процессе, обладая при этом высокой культурой работы с информацией и осознанно соблюдая установленные правила и оказывают содействие деятельности подразделения обеспечения информационной безопасности;

13) ***принцип гибкости системы защиты***, предусматривающий способность реагирования системы информационной безопасности на изменения внешней среды и внутренних условий деятельности НСК, к которым можно отнести:

– изменения организационной и штатной структуры НСК;

– корпоративную реструктуризацию, слияние и поглощение;

– изменение существующих или внедрение принципиально новых информационных систем;

– новые технические средства;

– новые виды деятельности; новые услуги, продукты;

14) ***принцип открытости алгоритмов и механизмов защиты***, состоящий из того, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем;

15) ***принцип простоты применения средств защиты***, означающий, что механизмы и методы защиты должны быть интуитивно понятны и просты в использовании;

16) ***принцип обоснованности и технической реализуемости***, означающий, что информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на уровне современных передовых технологий, обоснованы с точки зрения достижения заданного уровня информационной безопасности и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности;

17) ***специализация и профессионализм***, предполагающий привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и лицензию на право оказания услуг в этой области;

18) ***обязательность контроля***, предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Недостатки системы информационной безопасности, выявленные уполномоченными сотрудниками НСК или подразделением обеспечения информационной безопасности НСК должны немедленно доводиться до сведения руководителей соответствующего уровня и своевременно, оперативно устраняться.

Руководство НСК должно периодически получать отчеты, суммирующие все проблемы, выявленные в системе информационной безопасности.

5. Основные цели и задачи системы обеспечения информационной безопасности

Система информационной безопасности НСК предусматривает комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

Основными целями системы информационной безопасности НСК являются обеспечение:

1) защиты объектов и субъектов информационных отношений НСК от возможного нанесения им материального, физического, морального или иного

ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;

2) защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий;

3) защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи, посредством минимизации уровня операционного и других рисков (рисков нанесения урона репутации НСК, правовых рисков и т.д.)

Для достижения основной цели защиты и обеспечения указанных свойств информации система информационной безопасности НСК должна обеспечивать эффективное решение следующих задач:

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы НСК;

– ограничение доступа в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация, а также непосредственно к самим средствам информатизации и коммуникациям;

– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

– реализация разрешительной системы допуска исполнителей (пользователей, сотрудников НСК) к работам, документам и информации с целью защиты от вмешательства в процесс функционирования информационной системы НСК посторонних лиц;

– разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам НСК (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

– обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– защиту системы от внедрения несанкционированных программ, включая вредоносных программ;

– учет документов, информационных массивов, регистрация действий пользователей, служащих (сотрудников НСК), контроль за несанкционированным доступом и действиями пользователей, служащих

(сотрудников НСК) и посторонних лиц;

– реализация инфраструктуры с открытым ключом, криптографическая защита информации ограниченного пользования, обрабатываемой и передаваемой средствами вычислительной техники по открытым каналам связи;

– надежное хранение документов и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение, и обеспечивающее защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

III. Основные субъекты и объекты информационных отношений

6. Основные субъекты информационных отношений НСК

Субъектами информационных отношений при обеспечении информационной безопасности НСК являются:

1) НСК, как собственник информационных ресурсов;

2) подразделение обеспечения информационной безопасности, ответственное за организацию эффективного функционирования системы информационной безопасности НСК;

3) подведомственные подразделения и территориальные органы НСК, участвующие в информационном обмене;

4) руководство и сотрудники структурных, подведомственных подразделений и территориальных органов НСК, в соответствии с возложенными на них функциями и полномочиями;

5) юридические и физические лица (в том числе субъекты персональных данных), сведения о которых накапливаются, хранятся и обрабатываются в информационной системе НСК;

6) другие юридические и физические лица, задействованные в обеспечении выполнения НСК своих функций (консультанты, разработчики, организации, привлекаемые для оказания услуг и пр.).

7. Объекты защиты

Основными объектами системы информационной безопасности в НСК являются:

– информационные ресурсы с ограниченным доступом, составляющие информацию для служебного пользования (ДСП) или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы НСК, независимо от формы и вида ее представления;

– процессы обработки информации в информационной системе НСК, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей

системы, сотрудников НСК, использующих информационные ресурсы системы, а также осуществляющих техническое обслуживание системы;

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды НСК.

8. Структура, состав и размещение основных объектов защиты, информационной связи

Информационная среда НСК является распределенной структурой, объединяющей информационные подсистемы Центрального аппарата НСК, подведомственных подразделений и территориальных органов в единую информационную систему НСК.

К основным особенностям информационной среды НСК, относятся:

– широкая территориальная распределенность компонентов информационной системы;

– объединение в единую систему большого количества технических средств обработки и передачи информации;

– значительное расширение сферы использования автоматизированных систем обработки информации в НСК;

– большое разнообразие решаемых задач и типов, обрабатываемых данных, режимов автоматизированной статистической обработки информации;

– значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных;

– объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;

– необходимость обеспечения непрерывности функционирования НСК;

– разнообразие категорий пользователей системы.

В этих условиях резко возрастает уязвимость информации и одним из важнейших элементов информационной среды НСК становится корпоративная информационная система, в которой обрабатываются и накапливаются значительные объемы выводимой информации, используемой различными пользователями.

9. Категории информационных ресурсов, подлежащих защите

В НСК циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, секретная, персональные данные, индивидуальные данные, метаданные) и открытые сведения.

Защите подлежит вся информация и информационные ресурсы НСК, независимо от ее представления и местонахождения в информационной среде

НСК.

С учетом выявленных угроз безопасности информации НСК режим защиты должен формироваться как совокупность способов и мер защиты, циркулирующей в информационной среде НСК информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или держателям информации (НСК).

Данные, предназначенные для разработки, производства и распространения официальной статистики, статистического анализа и статистических услуг, включая все виды деятельности, регулируемые настоящим Законом, должны использоваться исключительно в статистических целях.

Индивидуальные данные, имеющиеся в распоряжении производителей официальной статистики (НСК и его структурных подразделений), не предоставляются государственным органам, органам местного самоуправления или международным организациям в целях расследования, надзора, судебного разбирательства, принятия административных решений или в других аналогичных целях, относящихся к физическим, юридическим лицам или домохозяйствам.

10. Основные права и функции подразделения обеспечения информационной безопасности НСК

Реализацию задач по организации эффективного функционирования системы информационной безопасности в НСК обеспечивает подразделение обеспечения информационной безопасности НСК, на которое возлагаются решение следующих основных задач:

– учет и анализ активов информационно-коммуникационных технологий;

– координация работ по созданию и развитию элементов инфраструктуры информационной безопасности;

– регистрация информационной системы в Реестре государственной инфраструктуры электронного управления;

– контроль за сохранностью эталонных копий программного обеспечения, исходных программных кодов (при их наличии), комплекса настроек лицензионного программного обеспечения, электронных копий технической документации элементов инфраструктуры электронного управления и информационной системы НСК;

– взаимодействие с уполномоченным государственным органом, операторами информационных систем, другими государственными органами, органами местного самоуправления, организациями, в части реализации проектов в сфере электронного управления и информационной безопасности;

– проведение в жизнь политики обеспечения информационной безопасности, формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы НСК;

– организация мероприятий и координация работ всех подразделений НСК по комплексной защите информации;

– проведение внутреннего аудита и анализ текущего состояния информационной безопасности НСК;

– контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Также к основным функциям данного подразделения в сфере обеспечения информационной безопасности НСК относятся:

– контроль исполнения требований технической документации по информационной безопасности (кибербезопасности);

– контроль за документальным оформлением информационной безопасности (кибербезопасности);

– подготовка решений по обеспечению конфиденциальности, доступности, целостности информационных данных;

– участие в приемке в эксплуатацию системы информационной безопасности;

– контроль за управлением активами в части обеспечения информационной безопасности (кибербезопасности);

– контроль правомерности использования программного обеспечения;

– контроль обеспечения функционирования установленных систем информационной безопасности;

– наблюдение за функционированием системы информационной безопасности;

– оказании методической помощи сотрудникам НСК в вопросах обеспечения информационной безопасности;

– контроль за действиями администраторов баз данных, серверов и сетевых устройств;

– контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с информацией;

– организация по указанию руководства НСК служебного расследования по фактам нарушения правил обращения с информацией и оборудованием;

– контроль за управлением рисками в сфере информационно-коммуникационных технологий;

– контроль за регистрацией событий информационной безопасности (кибербезопасности);

– организация внешнего аудита информационной безопасности (кибербезопасности);

– контроль соблюдения требований информационной безопасности (кибербезопасности) в НСК;

– принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

– сбор, накопление, систематизация и обработка информации по

вопросам информационной безопасности.

Организационно – правовой статус подразделения обеспечения информационной безопасности НСК основана на том, что:

– численность подразделения должна быть достаточной для выполнения всех перечисленных выше функций;

– сотрудники, занимающиеся обеспечением информационной безопасности НСК, не должны иметь других обязанностей, связанных с обеспечением функционирования технических компонентов информационной системы НСК;

– сотрудники подразделения обеспечения информационной безопасности НСК должны иметь право доступа во все помещения, где, установлены технические средства информационной системы НСК, и право прекращать обработку информации при наличии непосредственной угрозы для нее;

– руководителю подразделения должно иметь право запрещать включение новых компонентов информационной системы НСК в число действующих, если они не отвечают требованиям защиты информации и это может привести к серьезным последствиям в случае реализации значимых угроз безопасности информации;

– подразделению обеспечения информационной безопасности НСК должны обеспечиваться все условия, необходимые для выполнения своих функций.

Для решения задач, возложенных на нее, подразделение обеспечения информационной безопасности НСК:

– определяет необходимость разработки нормативных документов, касающихся вопросов обеспечения информационной безопасности (кибербезопасности), включая документы, регламентирующие деятельность пользователей информационной системы НСК в указанной области;

– может получать информацию от пользователей информационной системы НСК по любым аспектам применения информационных технологий в НСК;

– участвует в проработке технических решений по вопросам обеспечения информационной безопасности при проектировании и разработке новых информационных технологий;

– участвует в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению информационной безопасности;

– контролирует деятельность пользователей информационной системы НСК по вопросам обеспечения информационной безопасности;

– по мере необходимости осуществляет выездные проверки в отношении территориальных органов НСК по согласованию с руководством НСК.

IV. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

11. Основные пути и меры обеспечения решения задач системы информационной безопасности

Комплекс мер по формированию режима обеспечения информационной безопасности НСК включает:

1) установление в НСК организационно-правового режима обеспечения безопасности информации (разработку необходимых нормативных документов, работа с персоналом, правил делопроизводства);

2) организационные и программно-технические мероприятия по предупреждению несанкционированных действий (доступа) к информационным ресурсам корпоративной информационной системы НСК;

3) комплекс мероприятий по контролю функционирования средств и систем защиты информационных ресурсов ограниченного пользования после случайных или преднамеренных воздействий;

4) комплекс оперативных мероприятий подразделения обеспечения информационных технологий и безопасности НСК по предотвращению (выявлению) проникновения в НСК лиц, имеющих отношение к другим организационным структурам, не имеющим отношение к НСК;

5) комплекс мероприятий по обеспечению безопасной обработки и хранения данных.

Соответственно, реализация мер полноценно достигаются обеспечением:

– строгого учета всех подлежащих защите ресурсов информационной системы НСК (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журналирования действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

– полноты, реальной выполнимости и непротиворечивости требований организационно-распорядительных документов НСК по вопросам обеспечения безопасности информации;

– подготовки должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

– наделения каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам НСК;

– достаточно четких знаний и строго соблюдения всеми пользователями информационной системы НСК требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственности за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам НСК;

– непрерывного поддержания необходимого уровня защищенности элементов информационной среды НСК с обеспечением резервирования технических средств и дублирования массивов и носителей информации;

– применения физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективного контроля над соблюдением пользователями информационных ресурсов НСК требований, но обеспечению безопасности информации;

– юридической защиты интересов НСК при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий сотрудников НСК и сторонних лиц;

– доступности информации и связанных с ней ресурсов для авторизованных пользователей;

– исключения несанкционированного, в том числе случайного, доступа к информационным системам НСК, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, данных, представляющих служебную или государственную тайну, а также иных несанкционированных действий;

– предотвращение внедрения в корпоративную информационную систему НСК вредоносных программ;

– ограничения доступа к корпоративной информационной системе НСК в нерабочее время и выходные дни.

12. Организационно-правовой режим обеспечения защиты информации

К организационно – правовым мерам защиты информации относятся меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность сотрудников НСК, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Организационно-правовой режим предусматривает создание и поддержание правовой базы безопасности информации, в частности, разработку и принятие организационно-распорядительных документов:

1) Положения об служебной и государственной тайне.

Указанное Положение регламентирует организацию, порядок работы со сведениями, составляющими служебную и государственную тайну, персональными данными, индивидуальными данными, имеющиеся в распоряжении производителей официальной статистики, обязанности и ответственность сотрудников, допущенных к этим сведениям, порядок передачи материалов, содержащих сведения, составляющим служебную и государственную тайну, государственным и коммерческим учреждениям и

организациям.

2) Перечня сведений, составляющих служебную и государственную тайну.

Перечень определяет сведения, отнесенные к категориям конфиденциальных, информации ограниченного распространения, уровень и сроки обеспечения ограничений по доступу к защищаемой информации.

3) *Нормативных документов в области обеспечения информационной безопасности* (кибербезопасности), детализирующих требования Политики информационной безопасности НСК, рабочих форм, журналов, заявок, протоколов и других документов, включая электронные, используемые для регистрации и подтверждения выполненных процедур и работ.

4) Приказов и распоряжений по установлению режима безопасности информации:

- о допуске сотрудников к работе с конфиденциальной информацией, информацией ограниченного распространения;
- о назначении администраторов и лиц, ответственных за работу с конфиденциальной информацией, с информацией ограниченного распространения в корпоративной информационной системе НСК.

5) Инструкций и функциональных обязанностей сотрудников:

- по организации охранно-пропускного режима;
- по организации делопроизводства;
- по администрированию информационных ресурсов корпоративной информационной системы;
- другие нормативные документы.

13. Организационно-технические мероприятия по защите информации и информационных активов

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты информационной системы.

1) Для обеспечения защиты информационных активов подразделением обеспечения информационных технологий и безопасности НСК проводятся:

- инвентаризация активов;
- классификация и маркировка активов в соответствии с системой классификации, принятой в государственном органе, органе местного самоуправления, организации;
- закрепление активов за должностными лицами и определение меры их ответственности за реализацию мероприятий по управлению активов кибербезопасности;
- регламентация в технической документации по кибербезопасности порядка:
- использования и возврата активов;
- идентификации, классификации и маркировки активов.

2) С целью контроля событий нарушений информационной безопасности в НСК:

а) проводится мониторинг событий, связанных с нарушением информационной безопасности, и анализ результатов мониторинга;

б) регистрируются события, связанные с состоянием информационной безопасности, и выявляются нарушения путем анализа журналов регистрации событий, в том числе:

- журналов регистрации событий операционных систем;
- журналов регистрации событий систем управления базами данных;
- журналов регистрации событий антивирусной защиты;
- журналов регистрации событий прикладного программного обеспечения;
- журналов регистрации событий телекоммуникационного оборудования;
- журналов регистрации событий систем обнаружения и предотвращения атак на информационную систему;
- журналов регистрации событий системы управления контентом;

в) обеспечивается синхронизация времени журналов регистрации событий с инфраструктурой источника времени;

г) журналы регистрации событий хранятся в течение срока, указанного в технической документации по кибербезопасности, но не менее трех лет, и находятся в оперативном доступе не менее трех месяцев;

д) ведутся журналы регистрации событий создаваемого программного обеспечения в соответствии с форматами и типами записей, определенными в Правилах проведения мониторинга обеспечения информационной безопасности (кибербезопасности), защиты и безопасного функционирования элементов инфраструктуры НСК по электронному управлению, утверждаемых уполномоченным государственным органом;

е) обеспечивается защита журналов регистрации событий от вмешательства и неавторизированного доступа; не допускается наличие у системных администраторов полномочий на изменение, удаление и отключение журналов; для конфиденциальных информационных систем требуются создание и ведение резервного хранилища журналов;

ж) обеспечивается внедрение формализованной процедуры информирования об инцидентах кибербезопасности и реагирования на инциденты кибербезопасности.

3) С целью защиты критически важных процессов в государственных информационных системах НСК от внутренних и внешних угроз:

- разрабатывается, тестируется и реализуется План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;
- доводится до сведения сотрудников НСК Инструкция о порядке действий пользователей по реагированию на инциденты кибербезопасности и

во внештатных (кризисных) ситуациях, утверждаемых НСК.

План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации, подлежит регулярной актуализации.

4) Техническая документация по информационной безопасности (кибербезопасности) создается в виде документированных правил, процедур и руководящих принципов, которыми руководствуется НСК и его структурные подразделения в своей деятельности.

Техническая документация по кибербезопасности утверждается решением руководства НСК и доводится до сведения всех служащих – сотрудников НСК.

Техническая документация по информационной безопасности (кибербезопасности) пересматривается с целью анализа и актуализации изложенной в ней информации не реже одного раза в два года.

5) Функциональные обязанности по обеспечению информационной безопасности и обязательства по исполнению требований технической документации по информационной безопасности сотрудников НСК вносятся в должностные инструкции и/или условия трудового договора.

В технической документации по информационной безопасности также определяется содержание процедур при увольнении служащих (сотрудников НСК), имеющих обязательства в области обеспечения информационной безопасности.

При увольнении или внесении изменений в условия трудового договора права доступа служащего (сотрудника НСК) к информации и средствам обработки информации:

– включает физический и логический доступ, идентификаторы доступа, подписи, документации, которая идентифицирует его как действующего сотрудника НСК;

– аннулируется после прекращения его трудового договора или изменяются при внесении изменений в условия трудового договора.

6) В целях обеспечения информационной безопасности при эксплуатации государственных информационных систем и других объектов электронного управления в НСК устанавливаются требования к:

– способам идентификации;

– применяемым средствам криптографической защиты информации;

– способам обеспечения доступности и отказоустойчивости;

– мониторингу обеспечения информационной безопасности, защиты и безопасного функционирования;

– применению средств и систем обеспечения информационной безопасности;

– разрабатываемому или приобретаемому прикладному программному обеспечению предусматривают применение средств:

- идентификации и аутентификации пользователей, при необходимости электронной подписью, и регистрационных свидетельств;

- управления доступом;
- контроля целостности;
- журналирования действий пользователей, влияющих на кибербезопасность;
- защиты онлайновых транзакций;
- криптографической защиты информации с использованием средств криптографической защиты информации соответствующего уровня при хранении и обработке;
- журналирования критичных событий программного обеспечения;

7) На технические средства защиты возлагается решение также следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информацией, находящейся на нем.

14. Безопасная обработка и хранение данных

1. Структурные подразделения Центрального аппарата НСК, подведомственные подразделения и территориальные органы НСК, осуществляющие производство официальной статистики обязаны:

1) обеспечивать защиту индивидуальных данных;

2) обеспечивать защиту конфиденциальных агрегированных показателей и статистических данных до их выпуска;

3) принимать регулирующие, административные, технические и организационные меры по предупреждению доступа к данным со стороны неуполномоченных лиц.

2. Структурные подразделения Центрального аппарата НСК, подведомственные подразделения и территориальные органы НСК, осуществляющие производство официальной статистики, производят обработку и хранение индивидуальных данных с идентификаторами в течение периода, необходимого для достижения статистических целей, в соответствии с законодательством Кыргызской Республики в сфере персональных данных.

Идентификаторы, используемые в бумажных и электронных формах сбора данных и содержащиеся в административных данных, которые были переданы производителям официальной статистики в НСК, уничтожаются с момента отсутствия необходимости использования их в статистических целях по согласованию с поставщиками административных данных.

3. С целью защиты информации для служебного пользования, конфиденциальной информации, специальных категорий персональных данных, содержащихся в базах данных информационных систем, применяются средства криптографической защиты информации (программные или аппаратные) с параметрами согласно Техническим требованиям к средствам криптографической защиты информации, соответствующего уровня безопасности, установленного законодательством Кыргызской Республики.

15. Физическая охрана и режимные требования объектов информатизации

Физическая защита зданий, помещений, объектов и средств информатизации должна быть организована подразделением НСК по информационной безопасности посредством обеспечения установления соответствующих постов охраны, технических средств охраны или любых других способов, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

Физическая охрана объектов информатизации (компонентов информационной системы НСК) включает:

1) организацию системы охранно-пропускного режима и системы контроля допуска на объект;

2) введение дополнительных ограничений по доступу в помещения, предназначенные для хранения информации ограниченного пользования (кодовые и электронные замки, карточки допуска и т.д.);

3) визуальный и технический контроль контролируемой зоны объекта защиты; применение систем охранной и пожарной сигнализации.

Выполнение режимных требований при работе с информацией ограниченного пользования предполагает:

1) разграничение допуска к информационным ресурсам ограниченного пользования;

2) разграничение допуска к ресурсам корпоративной информационной системы;

3) ведение учета ознакомления сотрудников с информацией ограниченного пользования;

4) включение в функциональные обязанности сотрудников обязательства о неразглашении и сохранности сведений ограниченного пользования;

5) организация уничтожения информационных массивов данных, материальных носителей информации;

6) оборудование служебных помещений сейфами, шкафами для хранения бумажных и других носителей информации;

7) обеспечение акустической защиты помещений, в которых

обсуждается информация конфиденциального характера.

16. Мероприятия технического контроля

Для обеспечения информационной безопасности в НСК:

1) в технической документации по информационной безопасности (кибербезопасности) определяются и применяются при эксплуатации:

– правила установки, обновления и удаления программного обеспечения на серверах и рабочих станциях;

– процедуры управления изменениями и анализа прикладного программного обеспечения, в случае изменения системного программного обеспечения;

– способы размещения рабочих станций служащих (сотрудников НСК);

– способы защиты рабочих станций от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб;

– процедуры и периодичность технического обслуживания рабочих станций для обеспечения непрерывной доступности и целостности;

– способы защиты рабочих станций мобильных пользователей, находящихся за пределами НСК, с учетом различных внешних рисков;

– способы гарантированного уничтожения информации при повторном использовании рабочих станций или выводе из эксплуатации носителей информации;

– правила выноса рабочих станций за пределы рабочего места;

2) на регулярной основе проводится учет рабочих станций подразделением, компетентным в вопросах информационных технологий, с проверкой конфигураций;

3) лицензируемое программное обеспечение используется и приобретается только при условии наличия лицензии;

4) установка и применение на рабочих станциях программных или аппаратных средств удаленного управления извне локальной сетью внутреннего контура исключается; удаленное управление внутри локальной сети внутреннего контура допускается в случаях, прямо предусмотренных нормативным актом НСК, определяющим условия и порядок предоставления такого удаленного доступа (приказе, распоряжении, инструкции);

5) неиспользуемые порты ввода – вывода рабочих станций и мобильных компьютеров служащих (сотрудников НСК) отключаются или блокируются, за исключением рабочих станций сотрудников подразделения обеспечения информационной безопасности НСК.

6) С целью защиты информации для служебного пользования, конфиденциальной информации, специальных категорий персональных данных, содержащихся в базах данных информационных систем, применяются средства криптографической защиты информации (программные или аппаратные) с параметрами согласно установленным техническим требованиям к средствам криптографической защиты информации, соответствующего уровня безопасности.

17. Управление рисками/угрозами информационной безопасности

С целью управления рисками/угрозами в сфере информационной безопасности НСК осуществляются:

1) определение перечня угроз информационной безопасности (кибербезопасности) в информационных системах при осуществлении НСК соответствующих видов деятельности;

2) идентификация рисков в отношении перечня идентифицированных и классифицированных активов, включающая:

- выявление угроз информационной безопасности и их источников;
- выявление уязвимостей, которые могут привести к реализации угроз;
- определение каналов утечки информации;
- формирование модели нарушителя;

3) выбор критериев принятия идентифицированных рисков;

4) формирование каталога угроз (рисков) информационной безопасности, включая оценку (переоценку) угроз (рисков), определение потенциального ущерба;

5) разработка и утверждение мероприятия по нейтрализации или снижению угроз (рисков) информационной безопасности.

18. Регламентация доступа в помещения

Чувствительные к воздействиям компоненты информационной системы НСК должны размещаться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, серверов, реквизитов доступа и т.п.).

Серверное оборудование аппаратно-программного комплекса и системы хранения данных размещаются в серверном помещении. Серверное помещение располагается в отдельных, непроходных помещениях без оконных проемов. Серверное помещение надежно защищается от внешнего электромагнитного излучения. Обслуживание критически важного оборудования выполняется сертифицированным техническим персоналом.

Во время обработки информации ограниченного распространения в таких помещениях должен присутствовать только персонал сотрудников НСК, допущенный к работе с данной информацией. Запрещается прием посетителей в помещениях, когда осуществляется обработка информации ограниченного распространения.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

19. Регламентация допуска сотрудников к использованию информационных ресурсов

Допуск пользователей к работе с информационной системой НСК и доступ к ее ресурсам должен быть строго регламентирован.

Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламенту предоставления доступа к использованию информационных ресурсов НСК.

Основными пользователями информации в корпоративной информационной системе являются сотрудники структурных подразделений Центрального аппарата НСК, подведомственных подразделений и территориальных органов НСК.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с подразделением обеспечения информационной безопасности НСК;

– руководитель структурного подразделения НСК имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники НСК или других организаций, зарегистрированные как легальные пользователи информационной системы НСК и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы, информации ограниченного пользования.

Каждый сотрудник при приеме на работу должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению служебной и государственной тайны, информации персонального характера.

Обработка информации в компонентах информационной системы НСК должна производиться в соответствии с утвержденными инструкциями НСК, содержащие требования по обеспечению информационной безопасности.

20. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

Подлежащие защите ресурсы системы (документы, задачи, сервера, программы) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников НСК, с которых возможен доступ к ресурсам корпоративной информационной

системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

Все неиспользуемые в работе устройства ввода-вывода информации на рабочих местах сотрудников, работающих с конфиденциальной информацией, должны быть по возможности отключены, ненужные для работы программные средства и информационные данные на внешних материальных носителях информации должны быть удалены.

Дополнительные устройства обмена информацией могут использоваться только в исключительных случаях и только в качестве временного средства. Установка подобных устройств должна согласовываться с подразделением обеспечения информационной безопасности НСК.

В компонентах корпоративной информационной системы и на рабочих местах пользователей (сотрудников НСК) должны устанавливаться и использоваться программные средства, только получившие разрешение от подразделения информационной безопасности НСК.

Для решения специальных задач по оценке защищенности корпоративной информационной системы НСК и построении системы защиты информации в информационной системе НСК, может применяться специальное программное обеспечение, согласованное с подразделением обеспечения информационной безопасности НСК.

Контроль эффективности защиты информации 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.

Контроль может проводиться как подразделениями обеспечения информационной безопасности НСК, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

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

Оборудование корпоративной информационной системы, используемое для доступа к конфиденциальной информации, к которому доступ обслуживающего персонала сотрудников НСК в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам, должно закрываться и опечатываться (пломбироваться).

21. Подбор и подготовка персонала, обучение пользователей

Пользователи информационными данными информационной системы НСК, включая сотрудников структурных подразделений НСК (Центрального аппарата НСК, подведомственных подразделений и территориальных органов) должны быть ознакомлены со своим уровнем полномочий, а также организационно распорядительной, нормативной, технической документацией, определяющей требования и порядок обработки информации в НСК.

К нормам, обязательным для исполнения всеми, кто работает с информационными ресурсами НСК относятся запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационной системы НСК, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, субъектов информационных отношений, субъектов персональных данных.

Все пользователи данных внутренней информационной системы НСК должны быть ознакомлены с организационно – распорядительными документами по обеспечению информационной безопасности НСК, в части, их касающейся, должны знать и неукоснительно выполнять инструкции, и знать общие обязанности по обеспечению безопасности информации.

Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

22. Средства обеспечения информационной безопасности

Для обеспечения информационной безопасности НСК используются следующие средства защиты:

1) средства идентификации и аутентификации пользователей;

В целях предотвращения работы с ресурсами информационной системы НСК посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей).

Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);
- путем проверки знания ими паролей;
- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

2) средства разграничения доступа;

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию; в отдельные помещения;
- к компонентам информационной среды НСК и элементам системы защиты информации (физический доступ);
- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);
- к активным ресурсам (прикладным программам, задачам и т.п.);
- к операционной системе, системным программам и программам

защиты.

3) средства обеспечения и контроля целостности;

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронно-цифровой подписи; средствами учета;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

4) средства оперативного контроля и регистрации событий безопасности;

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение Политики и привести к возникновению кризисных ситуаций.

Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации.

Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);

– получения твердой копии (печати) журнала регистрации событий безопасности;

– упорядочения журналов, а также установления ограничений на срок их хранения;

– оперативного оповещения администратора безопасности о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация;

– дата и время события;

– идентификатор субъекта, осуществляющего регистрируемое действие;

– действие (тип доступа).

5) криптографические средства.

Основными элементами системы, обеспечения безопасности информации корпоративной информационной системы НСК являются криптографические

методы и средства защиты.

Перспективным направлением, использования криптографических методов, является создание инфраструктуры безопасности с использованием открытых ключей (PKI - Public Key Infrastructure).

Организация защищенного on-line взаимодействия удаленных территориальных органов НСК, дополнительных офисов и партнеров НСК на основе использования средств криптозащиты позволит:

– защитить конфиденциальную информацию НСК при ее передаче по каналам связи;

– защитить информационную систему (внутренние локальные вычислительные сети) Центрального аппарата НСК, подведомственных подразделений и территориальных органов от несанкционированных воздействий извне;

– сделать информационные взаимодействия НСК более эффективным за счет централизации управления ресурсами;

– оптимизировать затраты на администрирование сетей удаленных подразделений.

Конфиденциальность и защита информации при ее передаче, но каналам связи должна обеспечиваться также за счет применения средств абонентского шифрования.

В корпоративной информационной системе, являющейся структурой с распределенными информационными ресурсами, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений.

Средства защиты должны применяться ко всем чувствительным ресурсам информационной системы НСК, независимо от их вида и формы представления информации в них.

V. Заключительные положения

23. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы НСК

Любое грубое нарушение порядка и правил пользования информационными ресурсами НСК должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Мера ответственности пользователей информационных ресурсов НСК за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства НСК.

24. Внесении изменений и дополнений в Политику информационной безопасности НСК

Настоящая Политика утверждается Приказом Председателя НСК.

Изменения и дополнения в настоящую Политику вносятся по инициативе руководства НСК, руководителя подразделения обеспечения информационной безопасности НСК и утверждаются Приказом Председателя НСК.