«O`ZBEKISTON TEMIR YO`LLARI»
Davlat-aksiyadorlik temir
yo`l Kompaniyasi

Государственно–акционерная
железнодорожная компания
«УЗБЕКИСТОН ТЕМИР ЙУЛЛАРИ»

«СОГЛАСОВАНО»
Председатель Государственного комитета связи, информатизации и телекоммуникационных технологий

Мирзахидов Х.М. _____

"20" мая 2013 г.

«СОГЛАСОВАНО»
Начальник Государственной инспекции по надзору в сфере связи, информатизации и телекоммуникационных технологий

Умарходжаев Ф.Т. _____

"03" июня 2013 г.

«УТВЕРЖДЕНА»
Приказом Председателя Правления
ГАЖК «Узбекистон темир йуллари»
№204 -Н

" 24 " мая *2013* г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: *1.06.2013 г.*

Государственно-акционерная железнодорожная компании
«УЗБЕКИСТОН ТЕМИР ЙУЛЛАРИ»

Ташкент-2013

Предисловие

1 РАЗРАБОТАНА Управлением обеспечения информационной безопасности и информационного развития

2 ВНЕСЕНА Государственно−акционерной железнодорожной компанией «УЗБЕКИСТОН ТЕМИР ЙУЛЛАРИ»

3 УТВЕРЖДЕНА Приказом Председателя Правления ГАЖК «УЗБЕКИСТОН ТЕМИР ЙУЛЛАРИ» ***204-Н от 24 мая 2013 года***

4 ВВЕДЕНА ВПЕРВЫЕ

Содержание

АННОТАЦИЯ

Необходимость обеспечения информационной безопасности и защиты информационных ресурсов определяется двумя основными условиями:

– интересами собственника информационных ресурсов в защите своей собственности;

– интересами государства, общества и гражданина в защите своих интересов в информационной сфере.

Документированная информация, средства информатизации, информационные технологии и другие информационные ресурсы в настоящее время стали неотъемлемыми частями бизнес-процессов.

Разглашение сведений, отнесенных законодательством к конфиденциальной информации государства, организации или конкретного гражданина, также может нанести существенный ущерб ее владельцу. Поэтому государство требует обеспечить защиту конфиденциальной информации, всеми субъектами информационных отношений на всей территории Республики Узбекистан. Ответственность за несоблюдение этих требований определена в соответствующих законах.

Под информационной безопасностью организации понимается состояние защищенности ее информационной системы, включающей документированную информацию на всех видах носителей, программные и технические средства ее создания, тиражирования, хранения и обработки, формализованные процедуры обмена информацией между пользователями информационной системы, самих пользователей, речевую информацию.

Состояние защищенности информационной системы компании, как и любой другой организации, определяется по соответствию ряда параметров информационной системы определенным группам требований к безопасности, сформулированным в руководящих документах уполномоченных и контролирующих государственных органов, республиканских или международных стандартах по информационной безопасности.

Настоящий документ разработан на основе Концепции информационной безопасности ГАЖК «УТЙ» (Приказ №221-Н от 15.16.2009 г.) и международных стандартов O’z DSt ISO/IEC 13335-2009 "Управление безопасностью информационно-коммуникационных технологий ", O’z DSt ISO/IEC 15408-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», семейства стандартов O’z DSt ISO/IEC 27000 определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению, интегрирующего лучшие мировые практики управления информационной безопасностью.

Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на обеспечение информационной безопасности в информационных системах, включая бумажный документооборот и обмен речевой конфиденциальной информацией.

Политика информационной безопасности представляет пакет документов, включающих головной документ – «Политика информационной безопасности» и

документы, регламентирующие процессы обеспечения информационной безопасности, деятельность должностных лиц инфраструктуры информационной безопасности и пользователей информационно-коммуникационных систем ГАЖК.

Цель политики – выработать и утвердить единые требования и правила, способные обеспечить надлежащую защиту информации и бесперебойную работу информационных систем ГАЖК и свести к минимуму возможный ущерб от их эксплуатации посредством разработки эффективных превентивных и восстановительных мер противодействия угрозам безопасности.

Настоящая политика не противоречит требованиям действующего законодательства Республики Узбекистан и нормативных документов государственных органов, регламентирующих вопросы защиты информации и информационной безопасности.

АХБОРОТ ХАВФСИЗЛИГИ СИЁСАТИ
УМУМИЙ НИЗОМЛАР

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения ***1.06.2013 г.***

СПИСОК СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
ГАЖК	Государственная - акционерная железнодорожная компания
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационная технология
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
ПРД	Правила разграничения доступа
РД	Руководящий документ
РЖУ	Региональный железнодорожный узел
СВТ	Средства вычислительной техники
СЗИ	Система защиты информации
СКЗИ	Средства криптографической защиты информации
СКС	Структурированная кабельная система
СУБД	Система управления базами данных
ТЗ	Техническое задание на выполнение работ
ТУ	Технические указания
ЭВМ	Электронно-вычислительная машина
ЭЦП	Электронная цифровая подпись
ЦА	Центральный аппарат

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Нормативные ссылки

В настоящей Политике информационной безопасности использованы нормативные ссылки на следующие стандарты:

– ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

– O'z DSt ISO/IEC 12207:2007 Информационная технология. Процессы жизненного цикла программных средств

– O'z DSt ISO/IEC 13335-2009 Управление безопасностью информационно-коммуникационных технологий

– O'z DSt ISO/IEC 14764:2008 Разработка программного обеспечения. Процессы жизненного цикла программного обеспечения. Сопровождения программных средств (ISO/IEC 14764:2006, MOD)

– O'z DSt ISO/IEC 15408:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

– O'z DSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности системы управления информационной безопасностью. Требования (ISO/IEC 27001:2005,IDT)

– O'z DSt ISO/ IEC 27002:2008 Информационная технология. Методы обеспечения безопасности практические правила управления информационной безопасностью

– ИСО/МЭК 51:1999 "Аспекты безопасности. Руководящие указания по включению их в стандарты"

– ГОСТ ИСО 14001-98 Система управления окружающей средой. Требования и руководство по применению безопасности. Критерии оценки безопасности информационных технологий

– ISO 9001:2008, IDT Quality management systems

– ISO/IEC IS 13335-1ч 2Information Technology. Security techniques. Management of information and communications technology security

– ISO/IEC IS 15288-2002 Systems engineering. System Life Cycle Processes

– ISO/IEC TR 15504-1ч 5 Information technology. Process assessment

– ISO/IEC TR 18028-1ч 5 Information technology. Security techniques. IT network security

– ISO/IEC TR 18043 Information technology. Selection, deployment and operations of intrusion detection systems (IDS)

– ISO/IEC TR 18044-2004 Information Technology. Security techniques. Information security incident management

– ISO/IEC IS 17799-2005 (second edition) (с 2007 года — ISO/IEC IS 27002) Information Technology. Code of practice for information security management

1.2 Термины и определения

Автоматизированная система обработки информации - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, 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;

Авторизованный субъект доступа - субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия);

Администратор безопасности - лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты;

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

Безопасность информации - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования;

Безопасность информационной технологии - защищенность технологического процесса переработки информации;

Безопасность любого ресурса информационной системы - складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности;

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу);

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. Безопасность достигается проведением единой Концепции в области охраны и защиты важных ресурсов, системой мер

экономического, организационного и иного характера, адекватных угрозам жизненно важным интересам;

Внешний воздействующий фактор - воздействующий фактор, внешний по отношению к объекту информатизации;

Внутренний воздействующий фактор - воздействующий фактор, внутренний по отношению к объекту информатизации;

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

Выделенное помещение - помещение для размещения технических средств защищенного объекта информатизации, а также помещение, предназначенное для проведения семинаров, совещаний, бесед и других мероприятий, в котором циркулирует конфиденциальная речевая информация;

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

Доступ к информации - ознакомление с информацией или получение возможности ее обработки. Доступ к информации регламентируется ее правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществленный с нарушениями требований ее правового режима, рассматривается как несанкционированный доступ;

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 ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия;

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

Жизненно важные интересы - совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта.

Замысел защиты - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации и объекта;

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;

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

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

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта информация ограниченного распространения, передаваемая, хранимая, обрабатываемая или обсуждаемая в выделенных помещениях;

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

Информационные ресурсы - отдельные документы и отдельные массивы документов, 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 компании - организационно упорядоченная совокупность документов (массивов документов), независимо от формы их представления, и информационных технологий, в том числе с использованием вычислительной техники и связи. Информационная система компании включает в себя множество всех документов, существующих в компании;

Информационные способы нарушения безопасности информации включают:

−противозаконный сбор, распространение и использование информации;

−манипулирование информацией (дезинформация, сокрытие или искажение информации);

−незаконное копирование информации (данных и программ);

−незаконное уничтожение информации;

−хищение информации из баз и банков данных;

−нарушение адресности и оперативности информационного обмена;

−нарушение технологии обработки данных и информационного обмена.

Искусственные угрозы - это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

−непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;

−преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников);

Компьютерная информация - информация в виде:

−записей в памяти компьютеров, электронных устройствах, на машинных носителях (элементы, файлы, блоки, базы данных, микропрограммы, прикладные и

системные программы, пакеты и библиотеки программ, микросхемы, программно-информационные комплексы и др.), обеспечивающих функционирование объекта информатизации (сети);

−сообщений, передаваемых по сетям передачи данных;

−программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, представляемого непосредственно на экранах дисплеев, на внешних носителях данных (магнитные диски, магнитные ленты, оптические диски, дискеты, бумага для распечатки и т.п.) или через сети передачи данных;

−электронных записей о субъектах прав;

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей контролируемой зоны могут являться:

−периметр охраняемой территории ГАЖК;

−ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

−В отдельных случаях на период обработки техническими средствами секретной информации (проведения закрытого мероприятия) контролируемая зона временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне;

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 - автоматизированная система обработки информации ГАЖК;

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

Морально-этические меры защиты информации - традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний;

Нарушитель - это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке,

незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства;

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

Несанкционированный доступ - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

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.

Организационно-правовые способы нарушения безопасности информации включают:

−закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;

−невыполнение требований законодательства или нормативных актов и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области безопасности информации.

Организационные меры защиты - это 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;

Организационный контроль эффективности защиты информации - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите 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;

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе;

Правовые меры защиты информации - действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей;

Программно-математические способы нарушения безопасности информации включают:

−внедрение программ-вирусов;

−внедрение программных закладок как на стадии проектирования системы (в том числе путем заимствования "зараженного" закладками программного

продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

Радиоэлектронные способы нарушения безопасности информации включают:

−перехват информации в технических каналах ее утечки (побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации, наводок в коммуникациях (сети электропитания, заземления, радиотрансляции, пожарной и охранной сигнализации и т.д.) и линиях связи, путем прослушивания конфиденциальных разговоров с помощью акустических, виброакустических и лазерных технических средств разведки, прослушивания конфиденциальных телефонных разговоров, визуального наблюдения за работой средств отображения информации);

−перехват и дешифрование информации в сетях передачи данных и линиях связи;

−внедрение электронных устройств перехвата информации в технические средства и помещения;

−навязывание ложной информации по сетям передачи данных и линиям связи; радиоэлектронное подавление линий связи и систем управления.

Разграничение доступа к ресурсам - это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами;

Секретная информация - речевая информация, информация, циркулирующая в средствах вычислительной техники и связи, телекоммуникациях, а также другие информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, представленные в виде информативных акустических и электрических сигналов, физических полей, материальных носителей (в том числе на магнитной и оптической основе), информационных массивов и баз данных.

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 ГАЖК;

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;

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.);

Технология обеспечения информационной безопасности - определенное распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников ГАЖК по обеспечению комплексной защиты информационных ресурсов ГАЖК;

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;

Угроза интересам субъектов информационных отношений - потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие информационной системы может привести к нанесению ущерба интересам данных субъектов;

Уровень защиты (класс и категория защищенности) - характеристика, описываемая в нормативных документах определенной группой требований к данному классу и категории защищенности;

Уязвимость автоматизированной системы - любая характеристика автоматизированной системы, использование которой может привести к реализации угрозы;

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

Уязвимость субъекта информационных отношений - потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы обработки;

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;

Физические способы нарушения безопасности информации - включают:

−уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, целенаправленное внесение в них неисправностей;

−уничтожение, хищение и разрушение машинных или других оригиналов носителей информации;

−хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа;

−воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз безопасности информации;

−диверсионные действия по отношению к объектам безопасности информации (взрывы, поджоги, технические аварии и т.д.).

Физический 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;

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.

2 ПОЗИЦИЯ РУКОВОДСТВА ГАЖК

Информация и поддерживающие ее информационные системы и сети являются ценными производственными ресурсами. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения конкурентоспособности, движения денежной наличности, рентабельности, соответствия правовым нормам и имиджа ГАЖК.

Современные организации сталкиваются с возрастающей угрозой нарушения режима безопасности, исходящей от целого ряда источников. Информационным системам и сетям могут угрожать такие опасности, как компьютерное мошенничество, шпионаж, вандализм, а также другие источники отказов и аварий. Появляются все новые угрозы, способные нанести ущерб, такие, как компьютерные вирусы или хакеры. Предполагается, что такие угрозы информационной безопасности со временем станут более распространенными, опасными и изощренными.

Защитные меры оказываются значительно более дешевыми и эффективными, если они встроены в информационные системы и сервисы на стадиях задания требований и проектирования. Чем скорее принимаются меры по защите своих информационных систем, тем более дешевыми и эффективными они будут впоследствии. Поэтому:

– Руководство ГАЖК «Узбекистон темир йуллари» намерено обеспечивать надлежащую защиту информационных ресурсов ГАЖК и настоятельно требует от всех должностных лиц и сотрудников четкого соблюдения норм и правил, установленных в документах политики информационной безопасности;

– Руководством компании будет регулярно приниматься меры по решению проблем защиты информации, осуществлению контроля их выполнения, а также оказанию административной поддержки инициативам по обеспечению информационной безопасности;

– Все владельцы информационных ресурсов ГАЖК обязаны обеспечивать их защиту и имеют право требовать от руководства компании принятия действенных мер и выделения необходимых средств согласно требований документов политики информационной безопасности.

3. НАЗНАЧЕНИЕ И СТАТУС ДОКУМЕНТА

Настоящий документ является головным документом «Политики информационной безопасности ГАЖК «Узбекистон темир йуллари» (далее по тексту также «ГАЖК»), закрепляет основные организационные решения по управлению информационной безопасностью и определяет основные меры по защите информационных активов ГАЖК.

Документ описывает цели и задачи информационной безопасности, определяет совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется ГАЖК в своей деятельности, а также устанавливает должностных лиц, являющихся ответственными за реализацию политики ИБ и поддержание ее в актуальном состоянии.

Политика информационной безопасности ГАЖК (далее - Политика) учитывает современное состояние и ближайшие перспективы развития информационных технологий в ГАЖК, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений ГАЖК.

Основные положения и требования данного документа распространяются на все структурные подразделения ГАЖК. Основные вопросы Политики также распространяются на другие организации и учреждения, взаимодействующие с ГАЖК в качестве поставщиков и потребителей информационных ресурсов ГАЖК в том или ином качестве.

Для сотрудников компании требования данного документа, в части их касающейся, должны быть зафиксированы в их должностных обязанностях и соответствующих инструкциях.

Политика является методологической основой для:

−формирования и проведения единой политики в области обеспечения безопасности информации в ГАЖК;

−принятия управленческих решений и разработке практических мер по воплощению политика безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

−координации деятельности структурных подразделений ГАЖК при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;

−разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в ГАЖК.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности ГАЖК позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

4.КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ И БАЗОВЫЕ ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Законодательная и нормативная основа обеспечения информационной безопасности

Конфиденциальная информация, обрабатываемая в информационных системах ГАЖК, может содержать коммерческую тайну и (или) персональные данные сотрудников и клиентов компании. Поэтому она должна защищаться в соответствии с требованиями законодательства.

Кроме этого, информация, на основании которой осуществляется организация перевозочного процесса, предназначена только для внутреннего использования и может быть передана иным организациям только в соответствии с действующими нормативно-правовыми документами в сфере железнодорожного транспорта. Поэтому она должна защищаться в соответствии с ведомственными инструкциями.

Правовую основу защиты конфиденциальной информации в Республике Узбекистан составляют:

- Конституция Республики Узбекистан;
- Гражданский и Уголовный, Административный Кодексы Республики Узбекистан;
- Устав Государственно-акционерной железнодорожной компании «Узбекистон темир йуллари»;
- Законы Республики Узбекистан :
  - «О связи» от 13.01.1992г. №512-XII ;
  - «О телекоммуникациях» от 20.08.1999г. №822-I
  - «О принципах и гарантиях свободы информации» от 12.12.2002г. №439-II;
  - «Об информатизации» от 11.02.2003г. №560-II;
  - «Об электронной цифровой подписи» от 11.02.2003г. №562-II;
  - «Об электронном документообороте» от 29.04.2004г. №611-II;
  - «Об электронной коммерции» от 29.04.2004 г. №613-II;
  - «О гарантиях свободы предпринимательской деятельности» ;
  - «О защите государственных секретов» от 07.05.1993г. №848-XII;
  - «Об авторском праве и смежных правах»;
  - «О правовой охране программ для электронных вычислительных машин и баз данных» от 06.05.1994г. №1060-XII;
  - «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных» от 25.12.2007г. №ЗРУ-137;
- Указы и Постановления Президента Республики Узбекистан;

– Постановления Кабинета Министров Республики Узбекистан;

– Государственный стандарты в области развития информационных технологий и информационной безопасности .

– Международные договоры и соглашения, заключенные или признанные Республикой Узбекистан.

– «Перечень сведений, не подлежащих к опубликованию в открытой печати, передачи по радио, телевидению и сети Интернет» (ДСП -№14 СП\НР от 23.01.12 г.)

Нормативно-методическую базу, определяющую требования и рекомендации к защите информации в информационных системах, составляют руководящие документы Государственного комитета связи, информатизации и информационных технологий Республики Узбекистан, ГУП «Узинфоком», СНБ Республики Узбекистан, государственные и международные стандарты.

4.2 Концептуальные предпосылки информационной безопасности

Концепцией информационной безопасности (Приказ Председателя правления компании «УТИ» №221-Н от 15.06.09) устанавливаются следующие исходные методы в обеспечении информационной безопасности:

–В основе концептуальной схемы информационной безопасности ГАЖК лежит противоборство собственника[1] и злоумышленника[2] за контроль над информационными активами. Кроме этого рассматриваются незлоумышленные действия персонала ГАЖК, которые также могут привести к нарушению информационной безопасности и нанесению компании материального ущерба.

–Наибольшими возможностями для нанесения ущерба ГАЖК обладает его собственный персонал[3].

–Ответственность за собственный персонал несет непосредственно руководство управления, службы, подразделения, линейного предприятия, которому он относится.

–Собственник должен постоянно стремиться к выявлению следов активности. Для защиты своих интересов собственник создает уполномоченный орган – в качестве которого выступает Управление развития информационно-коммуникационных технологий и информационной безопасности, которое в свою очередь взаимодействует со службами, имеющие прямое отношение к информационным активам ГАЖК.

–Главный инструмент собственника – основанный на опыте прогноз

[1)] Под собственником здесь понимается субъект хозяйственной деятельности, имеющий права владения, распоряжения или пользования активами, который заинтересован или обязан (согласно требованиям законов или иных законодательных или нормативно-правовых актов) обеспечивать защиту активов от угроз, которые могут снизить их ценность или нанести ущерб собственнику.

[2)] Под злоумышленником здесь понимается лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий. Далее по тексту данные лица именуются злоумышленниками (нарушителями).

[3)] По данным международной статистики 80% нарушений информационной безопасности осуществляется сотрудниками предприятий и фирм и только 20% нарушений осуществляется от внешних источников угроз.

(составление модели угроз и модели нарушителя). Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

–Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ для собственника – разработать на основе точного прогноза политику ИБ и в соответствии с ней построить систему управления ИБ.

–Политика ИБ разрабатывается на основе принципов обеспечения ИБ, моделей угроз и нарушителей, идентификации активов, подлежащих защите, оценки рисков и с учетом особенностей и интересов конкретного собственника.

–Собственник должен знать, что он должен защищать. Собственник должен знать и уметь выделять (идентифицировать) наиболее важный для его бизнеса информационный актив (ресурс).

–Любые защитные меры в силу ряда объективных причин со временем имеют тенденцию к ослаблению своей эффективности, в результате чего общий уровень ИБ может снижаться. Это неминуемо ведет к возрастанию рисков ИБ. Для того чтобы этого не допустить, необходимо проводить регулярный мониторинг и аудит системы обеспечения ИБ и своевременно принимать меры по поддержанию эффективности системы управления ИБ на необходимом уровне.

4.3.Основные принципы обеспечения информационной безопасности

Построение системы, обеспечения безопасности информации ГАЖК, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

–законность;
–системность;
–комплексность;
–непрерывность;
–своевременность;
–преемственность и непрерывность совершенствования;
–разумная достаточность (экономическая целесообразность);
–персональная ответственность;
–минимизация полномочий;
–исключение конфликта интересов;
–взаимодействие и сотрудничество;
–гибкость системы защиты;
–открытость алгоритмов и механизмов защиты;
–простота применения средств защиты;
–обоснованность и техническая реализуемость;
–специализация и профессионализм;
–обязательность контроля.

4.3.1 Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации ГАЖК в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных подсистем.

Все пользователи информационной системы ГАЖК должны иметь представление об ответственности за правонарушения в области информации.

Реализация данного принципа необходима для защиты имени и репутации ГАЖК.

4.3.2 Системность

Системный подход к построению системы защиты информации в Банке предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации ГАЖК.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационной системы ГАЖК, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.3.3 Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.3.4 Непрерывность защиты

Обеспечение безопасности информации - процесс, осуществляемый Руководством ГАЖК, подразделениями защиты информации и сотрудниками всех

уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри ГАЖК и каждый сотрудник ГАЖК должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности ГАЖК. И ее эффективность зависит от участия руководства ГАЖК в обеспечении информационной безопасности.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

4.3.5 Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

4.3.6 Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы ГАЖК и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.3.7 Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационной системы ГАЖК. Излишние меры безопасности, помимо

экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

4.3.8 Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.3.9 Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

4.3.10 Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями ГАЖК. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение

неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

4.3.11 Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах структурных подразделений ГАЖК. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений защиты информации.

Важным элементом эффективной системы обеспечения безопасности информации в ГАЖК является высокая культура работы с информацией. Руководство ГАЖК несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, за создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности ГАЖК. Все сотрудники ГАЖК должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

4.3.12 Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Банком своей деятельности. В число таких изменений входят:

−изменения организационной и штатной структуры ГАЖК;

−корпоративная реструктуризация, слияния и поглощения;

−расширение или приобретение бизнеса за рубежом (включая влияние изменений в соответствующей экономической или правовой среде);

−изменение существующих или внедрение принципиально новых информационных систем;

−новые технические средства;

−новые виды деятельности; новые услуги, продукты.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

4.3.13 Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже

авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

4.3.14 Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

4.3.15 Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

4.3.16 Специализация и профессионализм

Предполагает 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 государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами ГАЖК (специалистами подразделений защиты информации).

4.3.17 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.

Контроль, за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, 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. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками ГАЖК или подразделениями обеспечения безопасности должны немедленно доводиться до сведения руководителей соответствующего уровня и оперативно устраняться. О существенных недостатках необходимо сообщать руководству ГАЖК. Важно, чтобы после получения информации соответствующие руководители обеспечивали своевременное исправление недостатков. Руководство должно периодически получать отчеты, суммирующие все проблемы, выявленные системой обеспечения информационной безопасности. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

4.4 Формирование режима обеспечения информационной безопасности

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

Комплекс мер по формированию режима обеспечения безопасности информации включает:

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

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

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

комплекс оперативных мероприятий подразделений безопасности по предотвращению (выявлению) проникновения в ГАЖК лиц, имеющих отношение к криминальным структурам.

Организационно-правовой режим предусматривает создание и поддержание правовой базы безопасности информации, в частности, разработку (введение в действие) следующих организационно-распорядительных документов:

Положение о коммерческой тайне. Указанное Положение регламентирует организацию, порядок работы со сведениями, составляющими коммерческую тайну ГАЖК, обязанности и ответственность сотрудников, допущенных к этим

сведениям, порядок передачи материалов, содержащих сведения, составляющим коммерческую тайну ГАЖК, государственным (коммерческим) учреждениям и организациям;

Перечень сведений, составляющих служебную и коммерческую тайну. Перечень определяет сведения, отнесенные к категориям конфиденциальных, уровень и сроки обеспечения ограничений по доступу к защищаемой информации;

Приказы и распоряжения по установлению режима безопасности информации:

допуске сотрудников к работе с информацией ограниченного распространения;

назначении администраторов и лиц, ответственных за работу с информацией ограниченного распространения в корпоративной информационной системе;

Инструкции и функциональные обязанности сотрудникам:

по организации охранно-пропускного режима;

по организации делопроизводства;

по администрированию информационных ресурсов корпоративной информационной системы;

другие нормативные документы.

Организационно-технические мероприятия по защите информации ограниченного распространения от утечки по техническим каналам предусматривают:

комплекс мер и соответствующих технических средств, ослабляющих утечку речевой и сигнальной информации - пассивная защита (защита);

комплекс мер и соответствующих технических средств, создающих помехи при съеме информации - активная защита (противодействие);

комплекс мер и соответствующих технических средств, позволяющих выявлять каналы утечки информации - поиск (обнаружение).

Физическая охрана объектов информатизации (компонентов Информационной системы ГАЖК) включает:

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

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

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

Выполнение режимных требований при работе с информацией ограниченного пользования предполагает:

разграничение допуска к информационным ресурсам ограниченного пользования; разграничение допуска к ресурсам корпоративной информационной системы;

ведение учета ознакомления сотрудников с информацией ограниченного пользования;

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

организация уничтожения информационных отходов (бумажных, магнитных и т.д.);

оборудование служебных помещений сейфами, шкафами для хранения бумажных и магнитных носителей информации.

Мероприятия технического контроля предусматривают:

контроль за проведением технического обслуживания, ремонта носителей информации и средств вычислительной техники;

проверки определенной части поступающего оборудования, предназначенного для обработки информации ограниченного пользования, на наличие специально внедренных закладных программ и устройств;

оборудование компонентов и подсистем корпоративной информационной системы устройствами защиты от сбоев электропитания и помех в линиях связи;

защита выделенных помещений при проведении закрытых (секретных) работ (переговоров);

постоянное обновление технических и программных средств защиты от несанкционированного доступа к информации в соответствие с меняющейся оперативной обстановкой.

5.ОБЪЕКТЫ ЗАЩИТЫ

Основными объектами системы информационной безопасности в ГАЖК являются:

−информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы ГАЖК, независимо от формы и вида ее представления;

−процессы обработки информации в информационной системе ГАЖК информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

−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.

5.1. Структура, состав и размещение основных объектов защиты, информационные связи

Информационная среда ГАЖК является распределенной структурой, объединяющей информационные подсистемы Центрального офиса и дополнительных офисов в единую информационную систему ГАЖК.

К основным особенностям информационной среды ГАЖК, относятся:

−широкая территориальная распределенность компонентов информационной системы;

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

−значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие и повсеместное распространение информационно-управляющих систем в ГАЖК;

−большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;

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

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

−абстрагирование владельцев данных от физических структур и места размещения данных (информации);

−наличие большого числа информационных каналов взаимодействия с "внешним миром" (источниками и потребителями информации);

−необходимость обеспечения непрерывности функционирования ГАЖК;

−высокая интенсивность информационных потоков;

−разнообразие категорий пользователей и обслуживающего персонала системы.

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

6. ЦЕЛИ И ЗАДАЧИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГАЖК

6.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении информационной безопасности ГАЖК являются:

−ГАЖК, как собственник информационных ресурсов;

−подразделения ГАЖК, участвующие в информационном обмене;

−руководство и сотрудники структурных подразделений ГАЖК, в соответствии с возложенными на них функциями;

−юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе ГАЖК;

−другие юридические и физические лица, задействованные в обеспечении выполнения ГАЖК своих функций (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

−своевременного доступа к необходимой им информации (ее доступности);

−достоверности (полноты, точности, адекватности, целостности) информации;

−конфиденциальности (сохранения в тайне) определенной части информации; защиты от навязывания им ложной (недостоверной, искаженной) информации;

−разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с информацией;

−возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

−защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

6.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений ГАЖК от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня операционного и других рисков (риск нанесения урона деловой репутации ГАЖК, правовой риск и т.д.).

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

−доступности информации для легальных пользователей (устойчивого функционирования информационной системы ГАЖК, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);

−целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационной системе ГАЖК и передаваемой по каналам связи;

−конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими множеству значимых угроз методами и средствами.

7. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Угрозы безопасности информации и их источники

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

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

Искусственные угрозы - это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

−непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;

−преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации ГАЖК являются:

−непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы ГАЖК (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

−преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам ГАЖК пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы ГАЖК;

−деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационной системы ГАЖК в целом и ее отдельных компонент;

−удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних сетей общего назначения (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;

−ошибки, допущенные при разработке компонентов информационной системы ГАЖК и их систем защиты, ошибки в программном обеспечении, отказы и сбои

технических средств (в том числе средств защиты информации и контроля эффективности защиты);

–аварии, стихийные бедствия.

Наиболее значимыми угрозами безопасности информации ГАЖК (способами нанесения ущерба субъектам информационных отношений) являются:

нарушение функциональности компонентов информационной системы ГАЖК, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов ГАЖК, а также фальсификация (подделка) документов;

нарушение конфиденциальности (разглашение, утечка) сведений, составляющих банковскую или коммерческую тайну, а также персональных данных

7.2. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации

Сотрудники ГАЖК, зарегистрированные как легальные пользователи информационной системы ГАЖК или обслуживающие ее компоненты, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и регламентов.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации ГАЖК (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

неумышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы ГАЖК или разрушению информационных или программно-технических ресурсов;

неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

разглашение, передача или утрата атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);

игнорирование организационных ограничений (установленных правил) при работе с информационными ресурсами;

проектирование архитектуры систем, технологий обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационной системы ГАЖК и безопасности информации;

пересылка данных и документов по ошибочному адресу (устройства);

ввод ошибочных данных;

неумышленная порча носителей информации;

неумышленное повреждение каналов связи;

неправомерное отключение оборудования или изменение режимов работы устройств или программ;

заражение компьютеров вирусами;

несанкционированный запуск технологических программ, способных вызвать потерю работоспособности компонентов Корпоративной информационной системы или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

некомпетентное использование, настройка или неправомерное отключение средств защиты.

7.3. Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода компонентов информационной системы ГАЖК из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

умышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы ГАЖК или разрушению информационных или программно-технических ресурсов;

действия по дезорганизации функционирования информационной системы ГАЖК; хищение документов и носителей информации;

несанкционированное копирование документов и носителей информации; умышленное искажение информации, ввод неверных данных;

отключение или вывод из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);

перехват данных, передаваемых по каналам связи и их анализ;

хищение производственных отходов (распечаток документов, записей, носителей информации и т.п.);

незаконное получение атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);

несанкционированный доступ к ресурсам Корпоративной информационной системы с рабочих станций легальных пользователей;

хищение или вскрытие шифров криптозащиты информации;

внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов корпоративной информационной системы ГАЖК;

незаконное использование оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;

применение подслушивающих устройств, дистанционная фото- и видео съемка для несанкционированного съема информации;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на технические

средства, непосредственно не участвующие в информационном обмене (сети питания).

7.4. Пути реализации основных естественных угроз безопасности информации

выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;

выход из строя или невозможность использования линий связи;

пожары, наводнения и другие стихийные бедствия.

7.5. Неформальная модель возможных нарушителей

Система обеспечения информационной безопасности ГАЖК должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

Некомпетентный (невнимательный) пользователь - сотрудник ГАЖК (или подразделения другой организации, являющийся легальным пользователем информационной системы ГАЖК), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства.

Любитель - сотрудник ГАЖК (или подразделения другого организации, являющийся зарегистрированным пользователем информационной системы ГАЖК), пытающийся нарушить систему защиты без корыстных целей или злого умысла или для самоутверждения. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.

Внутренний злоумышленник - сотрудник ГАЖК (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками ГАЖК. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне ГАЖК.

Внешний злоумышленник - постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне ГАЖК.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников ГАЖК:

−зарегистрированные пользователи информационной системы ГАЖК;

−сотрудники ГАЖК, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы ГАЖК, но имеющие доступ в здания и помещения;

−персонал, обслуживающий технические средства корпоративной информационной системы ГАЖК;

−сотрудники подразделений ГАЖК, задействованные в разработке и сопровождении программного обеспечения;

−сотрудники подразделений обеспечения безопасности ГАЖК;

−руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

−уволенные сотрудники ГАЖК;

−представители организаций, взаимодействующих по вопросам технического обеспечения ГАЖК;

−клиенты ГАЖК;

−посетители (представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);

−представители конкурирующих организаций;

−члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

−лица, случайно или умышленно проникшие в корпоративную информационную систему ГАЖК из внешних телекоммуникационных сетей (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников ГАЖК имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

Особую категорию составляют администраторы различных автоматизированных систем, имеющих практически неограниченный доступ к информационным ресурсам компонентов корпоративной информационной

системы. Численность данной категории пользователей должна быть минимальной, а их действия должны находится под обязательным контролем со стороны подразделений обеспечения информационной безопасности.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные во время работы в ГАЖК знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры являются наиболее агрессивным источником внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников ГАЖК всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками ГАЖК и криминальными структурами.

Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Конкурирующие организации, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к ресурсам информационной системы ГАЖК.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

нарушитель скрывает свои несанкционированные действия от других сотрудников ГАЖК;

несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, *хранения и передачи информации;

в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

7.6. Утечка информации по техническим каналам

При проведении мероприятий и эксплуатации технических средств возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

побочные электромагнитные излучения информативного сигнала от технических средств ГАЖК и линий передачи информации;

наводки информативного сигнала, обрабатываемого техническими средствами корпоративной информационной системы ГАЖК, на провода и линии, выходящие

за пределы контролируемой зоны ГАЖК, в т.ч. на цепи заземления и электропитания;

электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом;

радиоизлучения или электрические сигналы от внедренных в помещения ГАЖК специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом;

радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;

электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;

вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;

просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;

воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства ("закладки").

Перехват информации ограниченного распространения или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объектов ГАЖК, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими подразделений ГАЖК, а также с помощью скрытно устанавливаемой в районах важнейших объектов и на их территориях автономной автоматической аппаратуры.

В качестве аппаратуры разведок или воздействия на информацию и технические средства могут использоваться:

средства разведки для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций, и приема сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации ("закладок");

стационарные средства, размещаемые в зданиях;

портативные возимые и носимые средства, размещаемые в зданиях, в транспортных средствах, а также носимые лицами, ведущими разведку;

автономные автоматические средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

Стационарные средства обладают наибольшими энергетическими, техническими и функциональными возможностями. В то же время они, как правило, удалены от объектов защиты и не имеют возможности подключения к линиям, коммуникациям и сооружениям. Портативные средства могут использоваться непосредственно на объектах защиты или поблизости от них и могут подключаться к линиям и коммуникациям, выходящим за пределы контролируемой территории.

Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна в следствии:

- непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;
- случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;
- просмотра информации с экранов дисплеев и других средств ее отображения.

8. ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГАЖК

В качестве основных направлений обеспечения информационной безопасности ГАЖК рассматривается:

- Обеспечение информационной безопасности при ведении делопроизводства и осуществлении документооборота (как бумажного, так и электронного);
- Обеспечение информационной безопасности при обработке информации в автоматизированных и информационных системах;
- Обеспечение безопасности конфиденциальных переговоров;
- Обеспечение информационной безопасности при осуществлении взаимодействия с деловыми партнерами и клиентами;
- Обеспечение информационной безопасности при проведении работ по созданию (модернизации) информационных систем компании;
- Обеспечение информационной безопасности при соблюдении правовых и договорных требований;
- Обеспечение информационной безопасности в условиях чрезвычайных ситуаций.

8.1 Обеспечение информационной безопасности при осуществлении документооборота

Организация делопроизводства введется с соответствии с постановлением Кабинета Министров «об утверждении нормативных документов по делопроизводству и организации контроля исполнения в органах государственной власти и управления Республики Узбекистан» от 29.03.1999г. №140, Постановления Кабинета Министров «О мерах по укреплению исполнительской дисциплины» от 12.01.1999 г №12., Закона Республики Узбекистан «Об электронном документообороте» от 29.04.04 г. № 611-II., Законом Республики Узбекистан «О защите государственных секретов» от 7.05.1993г. №848-XII.Обеспечение информационной безопасности при ведении конфиденциального делопроизводства и осуществлении документооборота предполагает:

- организацию категорирования документов по степени их конфиденциальности, важности, доступности, срокам их необходимого хранения;
- организацию ведения делопроизводства и осуществления документооборота в соответствии с принятыми инструкциями, регламентами и правилами приема, передачи, регистрации, учета, визирования, копирования, контроля исполнения, надлежащего хранения, перевода в архив, уничтожения всех видов документов;
- обучение сотрудников принятым нормам и правилам работы с документами;
- организацию (совершенствование) разграничительной системы допуска сотрудников к документам различных степеней важности и средствам их обработки;
- обеспечение физической защиты доступа к местам хранения и обработки конфиденциальных документов;
- организацию системы контроля соблюдения правил обработки, хранения и уничтожения документов.

Общие правила представления информации, электронного и бумажного документооборота для сотрудников компании сводятся к следующим пунктам:

- представление информации или передача документов между подразделениями и сотрудниками компании осуществляется установленным (задокументированным) порядком;
- если порядок для конкретной информации или вида документа или информационного процесса не установлен, представление информации или передача документа сотрудником другому лицу может производиться только с разрешения руководителя соответствующего структурного подразделения;
- представление информации и документов в соответствующие государственные органы могут осуществлять только должностные лица и сотрудники компании, уполномоченные на это руководством, и совершать действия только в рамках полномочий, установленных в их должностных инструкциях;
- все документы, передаваемые во внешние организации, должны регистрироваться в ГАЖК как исходящие и иметь бумажные или электронные

копии, хранящиеся в делопроизводстве или в подразделениях, которые разрабатывают эти документы.

8.2. Обеспечение информационной безопасности автоматизированных систем

Обеспечение информационной безопасности в АС (O'z DSt ISO/IEC 15408-1,2,3) предполагает:

- определение владельцев информационных систем, отвечающих за санкционированный доступ к ним и их правильное использование;
- создание надежной системы идентификации и аутентификации пользователей, серверов и информационных ресурсов;
- организацию разграничительной системы допуска сотрудников к информационным ресурсам, системам и сервисам;
- обеспечение физической защиты доступа к серверному, коммуникационному и другому, критичному для функционирования АС, оборудованию и программному обеспечению;
- настройку и администрирование средств защиты в соответствии с принятой политикой безопасности;
- создание системы оперативного реагирования на события, таящие угрозу безопасности;
- обеспечение защиты информационных ресурсов АС при доступе к сетям общего пользования типа "Интернет";
- обучение сотрудников принятым нормам и правилам работы с информационными системами и информационными ресурсами;
- разработку и совершенствование нормативной базы, регламентирующей вопросы обеспечения эксплуатации, технического обслуживания, разделения процессов разработки и использования ПО, внедрения новых систем, модификации ПО, проверки целостности и работоспособности технических и программных средств информационных технологий и ряд других;
- организацию системы контроля достаточности и эффективности принимаемых мер защиты.

8.3. Обеспечение безопасности конфиденциальных переговоров

Обеспечение безопасности конфиденциальных переговоров предполагает:

- проведение защиты помещений, выделенных для проведения конфиденциальных переговоров, от утечки информации по акустическому и виброакустическому каналам;
- проведение защиты телефонных аппаратов и средств телефонной связи для возможности проведения конфиденциальных переговоров;
- организацию физической защиты и, если необходимо, охраны выделенных помещений, технических средств переговоров и установленных средств защиты;

- проверку выделенных помещений на предмет наличия закладных устройств несанкционированного съема и передачи информации ("жучков");
- разработку документов, регламентирующих проведение конфиденциальных переговоров при личных встречах и по каналам связи;
- организацию обучения сотрудников работе с установленными средствами защиты;
- организацию контроля уполномоченными специалистами принятых требований безопасности.

8.4. Обеспечение информационной безопасности при осуществлении взаимодействия с деловыми партнерами и клиентами

Обеспечение информационной безопасности при осуществлении взаимодействия компании с деловыми партнерами и клиентами предполагает:

- предварительный сбор, анализ и проверку информации о кредитоспособности, законопослушности и адекватности кандидата в деловые партнеры (проверка его по "черным" спискам, по выполнению его обязательств перед государственными контролирующими органами и его партнерами по другим договорам, и т.д.);
- заключение взаимного соглашения о неразглашении конфиденциальной информации при заключении договоров с юридическими лицами;
- формирование и контроль нормативно-правовых требований информационной безопасности, установленных в договорах о сотрудничестве, выполнении работ, предоставлении услуг;
- проведение юридической экспертизы соответствия заключаемых договоров действующему законодательству, региональным и государственным регламентирующим документам, в том числе, для иностранных партнеров - законодательству страны иностранного партнера и нормам международного права;
- контроль своевременности предоставления и правильности договорных и отчетных документов, а также документов отправляемых в адреса местных органов власти, хозяйствующих субъектов и деловых партнеров;
- обеспечение надлежащей защиты персональных данных сотрудников и клиентов.

Правила документооборота и представления информации при осуществлении сотрудничества с деловыми партнерами, в том числе иностранными, определяются в рамках подготовки договоров на выполнение работ, оказания услуг и т.д.

При необходимости допуска сотрудников сторонних организаций в ГАЖК или к сведениям, содержащим конфиденциальную информацию, в договорах должны присутствовать пункты, содержащие требования по неразглашению конфиденциальной информации, а также требования по соблюдению сотрудниками сторонних организаций установленного режима безопасности в ГАЖК.

Договорная документация должна обязательно проходить юридическую экспертизу на предмет соответствия требованиям безопасности ГАЖК и требованиям на соответствие договоров законодательству (и международному праву, для иностранных партнеров).

Должностные лица компании, ответственные за выполнение договоров со сторонними организациями, обязаны соблюдать меры безопасности, установленные в данном документе, а также строго контролировать соблюдение требований безопасности, установленных в договорной документации, сотрудниками сторонних организаций.

8.5. Обеспечение информационной безопасности при создании информационных систем компании

Обеспечение информационной безопасности при проведении работ по созданию (модернизации) информационных ресурсов и систем компании предполагает, что:

- требования к безопасности информационных систем (с учетом их важности и влияния на стоимость и скорость реализации) следует определить на стадии задания требований к проекту, а также обосновать, согласовать и документировать их в рамках общего плана работ по созданию автоматизированных систем. В случае невозможности определения таких требований на ранних этапах работ они должны быть сформулированы и реализованы в течение проекта или, в отдельных случаях, в рамках дополнительных подпроектов;
- отдельные требования по безопасности могут быть реализованы в рамках дополнительных подпроектов;
- необходимо провести анализ защищаемых ресурсов в рамках проекта и определить возможности использования различных средств контроля для предотвращения и выявления случаев нарушения защиты, а также восстановления работоспособности систем после их выхода из строя и инцидентов в системе безопасности;

При этом следует рассмотреть необходимость:

- управления доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- регистрации значительных событий в контрольном журнале для целей повседневного контроля или специальных расследований;
- проверки и обеспечения целостности жизненно важных данных на всех или избранных стадиях их обработки;
- защиты конфиденциальных данных от несанкционированного раскрытия, в том числе возможное использование средств шифрования данных;
- выполнения требований инструкций и действующего законодательства, а также договорных требований;
- снятия резервных копий с критически важных производственных данных;
- восстановления систем после их отказов, особенно для систем с повышенными требованиями к доступности;
- защиты систем от внесения несанкционированных дополнений и изменений;

- предоставления возможности безопасного управления системами и их использования сотрудникам;
- проектирование и эксплуатация систем должны соответствовать общепринятым промышленным стандартам обеспечения надежной защиты, определенным в государственных стандартах и международных правилах управления безопасностью;
- должна обеспечиваться безопасность в среде разработки и рабочей среде, в том числе определены процедуры управления процессом внесения изменений, технический анализ изменений, вносимых в операционную систему, ограничения на внесение изменений в пакеты программ и т.д.
- при внедрении новой системы должен быть регламентирован процесс утверждения информационных решений руководством.

8.6. Контроль выполнения правовых и договорных требований

Для того чтобы ГАЖК не понесла ущерба из-за несоблюдения каких-либо правовых и договорных требований должностные лица структурных подразделений обязаны осуществлять контроль их выполнения.

В соответствии с рекомендациями международного стандарта управления информационной безопасностью ISO/IEC 17799, - цель контроля выполнения правовых и договорных требований: - избежать нарушения правовых обязательств и обязательств по соблюдению уголовного и гражданского права, которым должны удовлетворять организации, взаимодействующие с ними хозяйствующие субъекты, деловые партнеры, клиенты, подрядчики и поставщики услуг при информационном взаимодействии.

Для достижения этой цели соответствующие должностные лица и владельцы информационных ресурсов при разработке, сопровождении и использовании информационных систем, должны определить в явном виде и задокументировать правовые и договорные требования к безопасности для каждой информационной системы. Для организации надлежащего контроля необходимо определить и задокументировать конкретные средства контроля, меры противодействия и обязанности для выполнения этих требований.

Контролю подлежат:

- правомочность копирования программного обеспечения, защищенного законом об авторском праве;
- защита документации ГАЖК;
- защита персональных данных сотрудников и клиентов ГАЖК;
- предотвращение незаконного использования информационных ресурсов ГАЖК.

Руководители структурных подразделений, в которых используются информационные системы, обязаны накладывать ограничения на копирование программ своими сотрудниками. Пользователи обязаны применять только те программы, которые разработаны или закуплены для информационных систем, или рекомендованное лицензионное программное обеспечение. Ответственность за организацию контроля несут руководители подразделений.

Важные для ГАЖК документы необходимо защищать от потери, уничтожения и подделки. Некоторые документы могут потребовать хранения в защищенном месте для удовлетворения правовых требований, а также для поддержки основных производственных работ. Примерами этого являются документы, которые могут потребоваться в качестве свидетельства того, что ГАЖК работает в соответствии с правовыми нормами, или для обеспечения надлежащей защиты от возможных гражданских или уголовных исков, или для подтверждения финансового состояния ГАЖК по отношению к партнерам, клиентам и аудиторам.

Руководители структурных подразделений компании обязаны обеспечить защиту персональных данных своих сотрудников и клиентов в соответствии с требованиями законодательства и государственных нормативно-технических документов. Ответственность за защиту от несанкционированного доступа, изменения, раскрытия и уничтожения, а также случайную потерю персональных данных несут владельцы информационных массивов и баз данных, где хранятся эти персональные данные.

Для предотвращения незаконного использования информационных ресурсов ГАЖК доступ к ним должен быть санкционирован руководителями подразделений, которые являются владельцами этих ресурсов. Использование этих ресурсов для целей, не связанных с основной работой ГАЖК или для несанкционированных целей без утверждения руководства и процедур учета следует рассматривать как незаконное использование информационных ресурсов. При выявлении таких случаев, их следует довести до сведения соответствующего руководства для наложения дисциплинарных взысканий. Все пользователи информационных систем получают письменную санкцию на доступ к информационным ресурсам, который им разрешается. Устанавливается, что доступ к информационным ресурсам, не указанным в санкции им запрещен.

8.7. Обеспечение информационной безопасности в условиях чрезвычайных ситуаций

Поскольку ни одна организация, в том числе и ГАЖК, не застрахованы от серьезных аварий, вызванных естественными причинами, чьим-то злым умыслом, халатностью, некомпетентностью или потерей предоставляемых услуг сторонними организациями, ГАЖК принимает меры для возможности выполнения своих критически важных функций, выполнение которых он хотел бы продолжать, несмотря ни на что.

Для защиты критически важных процессов от последствий крупных аварий и катастроф разрабатываются планы обеспечения бесперебойной работы ГАЖК. Должностные лица и сотрудники компании, ответственные за информационные ресурсы, обязаны предусматривать разработку и планирование превентивных и восстановительных мер по защите информационных активов компании, в части их касающейся.

Процесс планирования бесперебойной работы включает:

- идентификацию критически важных информационных ресурсов и систем компании и их ранжирование по приоритетам;

- определение возможного воздействия аварий различных типов на эти ресурсы;
- определение и согласование всех обязанностей должностных лиц и сотрудников компании, обслуживающих информационные ресурсы, и планов действий в чрезвычайных ситуациях;
- документирование согласованных процедур и процессов;
- надлежащую подготовку персонала к выполнению согласованных процедур и процессов в чрезвычайных ситуациях.

Планы обеспечения бесперебойной работы информационных ресурсов и систем должны включать:

- процедуры реагирования на чрезвычайные ситуации, описывающие меры, которые надлежит принять сразу после крупного инцидента, подвергающего опасности работу информационных систем и/или жизнь персонала;
- процедуры перехода на аварийный режим, описывающие меры, которые надлежит принять для временного перевода основных работ и сервисов в другие места;
- процедуры возобновления работы информационных систем, описывающие меры, которые надлежит принять для возобновления нормальной полноценной производственной деятельности ГАЖК на основном месте.

Все должностные лица и сотрудники компании должны четко знать и уметь выполнять свои обязанности, зафиксированные в планах обеспечения бесперебойной работы.

9. ОТВЕТСТВЕННОСТЬ ЗА ВЛАДЕНИЕ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ АКТИВОВ ГАЖК

Ответственность за обеспечение информационной безопасности и организацию надлежащей защиты информационных активов ГАЖК несут руководители подразделений, в чьем ведении находятся конкретные информационные активы.

Для однозначного определения владельцев информационных активов ГАЖК, их прав по разрешению доступа к ним сотрудников своего и других подразделений, определение ответственности за их сохранность – необходимо осуществить инвентаризацию и категорирование информационных ресурсов, и их закрепление за конкретными должностными лицами Приказами по компании.

9.1 Расследование инцидентов, связанных с нарушениями информационной безопасности

По каждому инциденту, связанному с нарушением информационной безопасности в компании, должно проводиться расследование. Ответственность за проведение расследования возлагается на руководителя подразделения компании, в котором оно произошло, а также на руководителей отделов системного

администрирования и информационной безопасности.

В результате расследования необходимо определить:

- нарушителя (нарушителей) информационной безопасности;
- категорию нарушения и величину нанесенного ущерба (если он есть);
- причины, приведшие к нарушению;
- меры и средства, необходимые для ликвидации нежелательных последствий;
- меры и средства, необходимые для ликвидации или ослабления причин, приведших к нарушению, чтобы подобные нарушения не повторялись в будущем.

Результаты расследования должны оформляться документально. Вид нарушения, если такового не было ранее, должен быть включен в перечень категорированных нарушений по информационной безопасности. К виновникам нарушений должны применяться административные или уголовные меры воздействия, соответствующие тяжести нарушения.

9.2 Ответственность за нарушение требований обеспечения информационной безопасности

Ответственность за нарушение требований обеспечения информационной безопасности накладывается на сотрудников компании, совершивших нарушения, в зависимости от категории нарушения, возникшего в результате необеспечения или нарушения информационной безопасности, и величины причиненного ущерба (нежелательных последствий).

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей, ключей на различной физической основе, биометрических характеристик личности и т.п.;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

Должностные лица и сотрудники компании могут привлекаться к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Республики Узбекистан и административно-правовыми нормами, установленными в ГАЖК.

10. ОСНОВНЫЕ МЕХАНИЗМЫ БЕЗОПАСНОСТИ, ИСПОЛЬЗУЕМЫЕ В АС

Для обеспечения защиты АС могут применяться следующие механизмы безопасности:

10.1.Аутентификация

Аутентификация (authentication) пользователей может осуществляться на основе применения одного или нескольких из следующих механизмов безопасности:

- аутентификации на основе паролей;
- использования протоколов запрос-ответ с использованием серверов авторизации;
- аутентификации на основе физического владения идентификатором;
- аутентификации на основе физических свойств пользователя;
- аутентификации с использованием доверенной внешней аутентификации;
- использования систем с обратным дозвоном.

В качестве средств идентификации могут применяться различного рода устройства: магнитные карточки, электронные ключи, считыватели отпечатков пальцев, радужной оболочки глаз и т.п.

10.2. Обеспечение конфиденциальности

Обеспечение конфиденциальности (confidentiality) информации может осуществляться на основе применения механизмов:

- абонентского шифрования блоков данных и файлов;
- проходного шифрования трафика сети;
- контроля содержимого (e-mail, http, ftp и т.д.);
- реализации системы инженерно-технической защиты (охрана, двери с замками, сейфы, контейнеры и т.д.) помещений, средств информатизации и носителей информации;
- отключения/удаления локальных устройств ввода/вывода информации;
- отключения/удаления неиспользуемых сервисов операционных систем и общего программного обеспечения;
- использования сертифицированных средств защиты, в том числе программного обеспечения на отсутствие недекларированных возможностей.

Надежность защиты конфиденциальной информации при ее хранении и передаче в АС может быть обеспечена за счет применения комплекса средств абонентского и канального шифрования. Ключевая система применяемых шифровальных средств должна обеспечивать криптографическую живучесть и многоуровневую защиту от компрометации ключевой информации.

10.3 Обеспечение неотказуемости

Обеспечение неотказуемости (non-repudiation) от переданных электронных документов может осуществляться на основе применения механизмов:

- электронной цифровой подписи;
- ведения журналов приема/передачи электронных документов;
- установления временных меток.

10.4 Обеспечение целостности

Обеспечение целостности (integrity) информации и программного обеспечения может осуществляться на основе применения механизмов:

- резервирования/восстановления программного обеспечения и данных;
- физического контроля доступа к техническим ресурсам;
- отключения/удаления локальных устройств ввода/вывода информации;
- использования антивирусных средств;
- хеширования.

Для обеспечения неизменности программной среды могут быть использованы механизмы контроля целостности программных и информационных файлов. Контроль их целостности может обеспечиваться:

- средствами подсчета контрольных сумм;
- средствами мониторинга динамики значений параметров программных объектов;
- средствами электронной цифровой подписи;
- средствами сравнения критичных ресурсов с их эталонными копиями;
- средствами разграничения доступа.

Для защиты систем от воздействия компьютерных вирусов необходимо использовать специальные антивирусные средства.

10.5. Контроль доступа

Контроль доступа (access Control) к ресурсам может обеспечиваться на основе применения механизмов:

- ведения списков контроля доступа;
- определения матрицы доступа;
- мандатного доступа;
- ролевого доступа;
- физического контроля доступа;
- идентификации;
- использования систем обратного дозвона;
- использования межсетевого экранирования на пакетном, транспортном и прикладном уровнях;
- использования трансляции сетевых адресов;
- контроль содержимого (e-mail, http, ftp и т.д.);
- аутентификации на основе обладания информацией, физического владения ресурсом или физических свойств абонента;
- использования внешних доверенных серверов авторизации;

Средствами контроля доступа должна обеспечиваться аутентификация пользователя системы (удостоверения, что пользователь является тем, за кого он себя выдает) и его авторизация (определение набора его прав и привилегий по доступу и использованию данных, программ, системных ресурсов и т.п.).

10.6 Обеспечение доступности

Обеспечение доступности ресурсов (availability) может осуществляться на основе применения механизмов:

- холодного и горячего резервирования, в том числе реализации катастрофоустойчивой схемы для бизнеса ГАЖК важнейших программно-аппаратных комплексов;
- кластеризации;
- резервирования программного обеспечения и данных;
- создания резервных источников электропитания;
- назначения приоритетов доступа.

10.7 Мониторинг и аудит

Мониторинг и аудит (monitoring and audit) может проводиться на основе применения механизмов:

- регистрации доступа (чтение, запись, удаление, создание) к данным;
- регистрации запуска процессов;
- регистрации статуса выполненной операции (удачно/неудачно);
- регистрации операций администрирования;
- регистрации изменения привилегий и прав доступа;
- регистрации вывода информации на печать и внешние носители;
- оперативного (on-line) уведомления об НСД;
- анализа сетевого трафика;
- анализа системной активности;
- регистрации входа (выхода) в систему.

Средства мониторинга и аудита должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций.

10.8 Управление информационной безопасностью

Управление информационной безопасностью (security management) должно осуществляться на основе применения механизмов:

- централизованного или децентрализованного хранения аутентификационной информации;
- централизованного или децентрализованного хранения авторизационной информации;
- централизованного управления параметрами компонентов подсистемы информационной безопасности.

Средства управления информационной безопасностью должны поддерживать следующие основные способы реагирования на обнаруженные факты НСД:

- извещение владельца информации о попытке НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- извещение администратора информационной безопасности;
- отключение терминала (рабочей станции), с которого были осуществлены попытки НСД к информации;
- блокирования межсетевого экрана;
- исключение нарушителя из списка зарегистрированных пользователей;

- подачу сигнала тревоги и др.

11 МЕРЫ ПО ОБЕСПЕЧЕНИЮ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1 Работа с персоналом по обеспечению информационной безопасности

11.1.1 Подбор персонала на должности, связанные с обработкой конфиденциальной информации

При подборе персонала на должности, связанные с обработкой конфиденциальной информации, все кандидаты на занятие подобных вакансий проверяются по следующим пунктам:

- наличие как минимум двух положительных характеристик, одна деловых и одна личных качеств;
- проверка (полноты и точности) сведений, сообщенных претендентом на вакансию в своей автобиографии;
- подтверждение академических степеней и профессиональной квалификации;
- проверка идентификации (паспортных данных);
- проверка благосостояния и выявление социальных проблем кандидата и его семьи.

Для практической проверки деловых качеств кандидата ему устанавливается трехмесячный испытательный срок с ограниченным допуском в это время к конфиденциальной информации.

11.1.2 Подписание с сотрудником Соглашения о конфиденциальности

Все кандидаты, претендующие на должности в ГАЖК, связанные с допуском к конфиденциальной информации, обязаны подписать обязательство о конфиденциальности (неразглашении конфиденциальной информации), прежде чем они приступят к исполнению должности.

Пользователи из сторонних организаций, которым необходимо работать в ГАЖК и которые не подпадают под действие существующего со сторонней организацией договора, содержащего обязательство о неразглашении, должны подписать личное обязательство о неразглашении, прежде чем им будет предоставлен доступ к информационным ресурсам компании.

Обязательства о неразглашении должны пересматриваться, когда изменяются условия найма сотрудников или договор с внешней организацией.

Ответственность за принятие кандидатом обязательства о конфиденциальности несут руководитель подразделения, в которое назначается сотрудник, и начальник отдела информационной безопасности.

11.1.3 Определение правил обеспечения информационной безопасности в должностных инструкциях

Руководители структурных подразделений компании, в которых обрабатывается конфиденциальная информация и осуществляется доступ к защищаемым ресурсам, совместно с сотрудниками отдела информационной безопасности обязаны обеспечивать включение в должностные инструкции сотрудников необходимые аспекты, связанные с информационной безопасностью исполняемой должности, и контролировать их соблюдение в течение всего времени работы данного сотрудника. Определение правил обеспечения ИБ в должностных инструкциях должно осуществляться в строгом соответствии с Концепцией и Политикой ИБ ГАЖК, а так же нормативно-законодательными документами и государственными стандартами РУз в области ИБ.

В инструкциях необходимо отражать общую ответственность за проведение в жизнь политики безопасности ГАЖК и конкретные обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите, связанных с исполнением должности.

Сотрудники отдела информационной безопасности обязаны периодически контролировать наличие и актуальное состояние необходимых аспектов информационной безопасности в должностных инструкциях.

11.1.4 Обучение сотрудников правилам информационной безопасности

При вступлении в должность нового сотрудника непосредственный руководитель подразделения компании, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования информационной безопасности в компании, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем в конкретном подразделении.

Сотрудника необходимо ознакомить со сведениями о политике информационной безопасности компании, принятых процедурах работы с документами и информационными ресурсами, правилами доступа к информационным системам и сервисам, а также, в письменной форме предоставить, разрешенный ему доступ (права и ограничения) к информационным ресурсам.

Сотрудник должен быть проинформирован об угрозах нарушения режима информационной безопасности и ответственности за его нарушение. Он должен быть ознакомлен с перечнем категорированных нарушений информационной безопасности и утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые в компании политику и процедуры безопасности.

Отдел информационной безопасности обязан проверить знания сотрудника по вопросам обеспечения информационной безопасности, требуемым на занимаемой должности, и разрешить ему допуск к исполнению должности, если его знания соответствуют установленному в компании уровню.

11.1.5 Правила использования рабочего стола и персонального компьютера

Для обеспечения установленного режима информационной безопасности в компании определяются правила использования рабочего стола и персонального компьютера, которые направлены на уменьшение риска несанкционированного доступа, хищения, потери и повреждения бумажных и электронных документов и дискет в рабочее и нерабочее время.

Сотрудники компании обязаны выполнять следующие рекомендации:

–Бумажная документация и дискеты, когда они не используются, особенно в нерабочее время, должны храниться в специально отведенных местах.

–Носители с конфиденциальной или критически важной производственной информацией, когда она не используется, должны храниться отдельно от общедоступной информации в надежных хранилищах (шкафах, сейфах), имеющих приспособления для опечатывания.

–Необходимо обеспечить защиту входящей и исходящей почты.

11.1.6 Правила реагирования сотрудника на события, несущие угрозу безопасности

Для своевременной и адекватной реакции на выявленные нарушения информационной безопасности, в компании должны быть разработаны правила и формальная процедура уведомления, описывающая действия сотрудника, которые ему надлежит принять при обнаружении инцидента в системе безопасности.

Правила регламентируют:

- перечень категорированных нарушений, которые требуют обязательной реакции;
- действия сотрудника по регистрации выявленного нарушения и сбора необходимой информации для аргументированного уведомления о нарушении;
- действия сотрудника по продолжению или аварийному прекращению процесса использования информационной системы;
- действия сотрудника по уведомлению ответственного лица за реакцию на угрозы безопасности;
- действия сотрудника, которые ему надлежит выполнить или запрещено выполнять, после уведомления ответственного лица за реакцию на угрозы безопасности.

За разработку и сопровождение общей части правил отвечает Управление НИБ. За организацию разработки и сопровождения правил, связанных с использование конкретных информационных систем в конкретном подразделении отвечает руководитель подразделения. За организацию разработки и сопровождения, частных правил, связанных с использованием общекорпоративных информационных систем отвечает отдел администрирования информационных технологий.

11.1.7 Обязанность уведомления об обнаруженных инцидентах в системе безопасности

Все сотрудники и подрядчики компании должны быть ознакомлены с правилами и процедурой уведомления о различных типах инцидентов, которые могут повлиять на безопасность его информационных ресурсов.

Все сотрудники компании обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях такого рода, а также о выявленных ими событиях, затрагивающих безопасность ГАЖК, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности. Закрепленные лица должны ежемесячно предоставлять отчет об инцидентах нарушений ИБ в подразделении в управление НИБ, для мониторинга и анализа, и разработки мер по их устранению.

11.1.8 Обязанность уведомления об обнаруженных слабых местах в системе безопасности

Сотрудники компании, являющиеся пользователями информационных систем и сервисов, обязаны регистрировать любые наблюдаемые или предполагаемые уязвимости (слабости) в системе безопасности, либо угрозы системам или сервисам и сообщать о них установленным порядком своему непосредственному руководству и поставщикам соответствующих услуг.

11.2 Меры по обеспечению безопасности речевой информации

Для обеспечения безопасности конфиденциальной речевой информации в ГАЖК принимаются организационные, организационно-технические и режимные меры. Организационные меры регламентируют правила передачи конфиденциальной речевой информации между сотрудниками внутри компании и при их взаимодействии с внешними организациями. Режимные меры обеспечивают подготовку проведения мероприятий, на которых будут раскрываться конфиденциальные сведения, выявление и нейтрализацию оперативных каналов утечки информации и контроль соблюдения принятых мер по обеспечению безопасности речевой информации. Организационно-технические меры обеспечивают защиту голосовой конфиденциальной информации при помощи использования технических и программных средств защиты.

Организационно-технические меры обеспечения безопасности конфиденциальной речевой информации предусматривают:

- оборудование рабочих кабинетов, переговорных комнат и помещений где проводятся совещания, на которых могут произноситься конфиденциальные сведения, средствами защиты от утечки информации по акустическому и виброакустическому каналам;

Ответственность за реализацию организационно-технических мер возлагается на руководителей подразделений, обеспечивающих эксплуатацию защищаемых помещений и технических систем обмена голосовой информацией.

Ответственность за обеспечение безопасности конфиденциальной информации при проведении переговоров возлагается на должностное лицо или сотрудника компании, передающего конфиденциальную информацию. При этом он обязан:

- знать перечень сведений, составляющих коммерческую тайну, а также порядок работы с документами, содержащими коммерческую тайну;
- передавать конфиденциальную информацию, получаемую в рамках своей производственной деятельности, только тем сотрудникам и в том объеме, которые определены в рамках его должностной инструкции;
- при передаче информации соблюдать установленные меры безопасности и режима (использовать защищаемые помещения, защищенные телефонные аппараты, установленные места, регламент, процедуры и т.п.);
- спрашивать и получать разрешение у своего непосредственного руководителя на передачу конкретных конфиденциальных сведений конкретному лицу в тех случаях, когда регламент передачи информации не определен или когда у сотрудника возникли какие-либо сомнения по поводу передачи конфиденциальной информации.

Сотруднику категорически запрещается:

- передавать конфиденциальную информацию какому-либо лицу вне рамок его производственной деятельности и должностных инструкций;
- нарушать установленные правила и регламенты передачи конфиденциальных сведений;
- отключать или блокировать установленные средства защиты.

Ответственность за режимное обеспечение проведения конфиденциальных совещаний и мероприятий возлагается на службу безопасности. В обязанности службы безопасности входят:

- проверка помещений, где будут проводиться конфиденциальные мероприятия на наличие посторонних предметов, в которых могут находиться закладные передающие устройства несанкционированного съема информации;
- обеспечение пропускного режима, встреча и сопровождение гостей в помещения для совещаний при приеме посетителей из внешних организаций;
- контроль соблюдения требований политики безопасности и регламентирующих документов по обеспечению информационной безопасности компании;
- проведение специальных проверок сувенирной продукции и подарков в адрес должностных лиц компании (входной контроль) на предмет обнаружения в них возможно внедренных электронных средств съема информации;
- временное изъятие или блокирование мобильных телефонов и звукозаписывающей аппаратуры у участников мероприятий при обсуждении особо важных для компании сведений;
- контроль своевременного ухода из компании посетителей из внешних организаций после окончания конфиденциальных мероприятий;
- организация проведения периодических проверок помещений, предназначенных для проведения конфиденциальных мероприятий, с целью выявления и нейтрализации возможных технических каналов утечки информации, способов несанкционированного доступа, несанкционированных и непреднамеренных воздействий.

11.3 Меры по обеспечению информационной безопасности в АС

11.3.1 Управление доступом

Для обеспечения информационной безопасности в АС и защиты от несанкционированного доступа к производственной информации, компьютерным системам и сервисам организовано управление доступом к информационным системам, приложениям, персональным компьютерам и рабочим станциям пользователей.

Пользователям прикладных систем, в том числе обслуживающему персоналу, следует предоставлять доступ к данным и приложениям в соответствии с обеспечением ***ролей*****,** возложенных на них.

Организацию управления доступом к сетевым ресурсам осуществляет отдел администрирования и отдел информационной безопасности.

Каждый владелец информационной системы должен четко сформулировать требования и формальные процедуры, необходимые для организации допуска сотрудников структурных подразделений к информационной системе, за правильное использование которой он несет персональную ответственность.

Руководители структурных подразделений обязаны определить необходимые потребности в информационных ресурсах и сервисах и сформулировать производственные требования по доступу сотрудников своих подразделений к информационным системам и ресурсам АС.

Для предотвращения несанкционированного доступа сотрудников к компьютерным системам АС должны быть разработаны формальные процедуры предоставления прав доступа к информационным системам.

Процедуры должны включать в себя все стадии жизненного цикла управления доступом пользователей – от начальной регистрации новых пользователей до удаления учетных записей пользователей, которые больше не нуждаются в доступе к информационным сервисам. Процедуры должны обеспечивать:

- проверку, предоставлено ли пользователю разрешение на использование сервиса владельцем системы;
- проверку, достаточен ли уровень доступа к системе, предоставленного пользователю, для выполнения возложенных на него производственных функций и не противоречит ли он политике безопасности;
- предоставление пользователям их права доступа в письменном виде;
- требование от пользователей подписания обязательства, чтобы показать, что они понимают условия доступа;
- требование от поставщиков услуг, чтобы они не предоставляли доступ к системам до тех пор, пока не будут закончены процедуры определения полномочий;
- ведение формального учета всех зарегистрированных лиц, использующих систему;
- изъятие права доступа у тех пользователей, которые сменили должность или покинули ГАЖК;

- периодическую проверку и удаление пользовательских идентификаторов и учетных записей, которые больше не требуются;
- проверку, не выданы ли пользовательские идентификаторы, которые больше не нужны, другим пользователям.

Необходимо ограничить и тщательно контролировать использование системных утилит администрирования прикладных систем, способных обойти средства контроля системы и приложений.

Предлагается использовать следующие способы защиты:

- защиту системных утилит с помощью паролей;
- изоляцию системных утилит от прикладного программного обеспечения;
- предоставление доступа к системным утилитам минимальному числу зарегистрированных пользователей;
- ограничение времени доступности системных утилит, например, временем внесения санкционированного изменения;
- регистрацию всех случаев использования системных утилит;
- определение и документирование уровней полномочий доступа к системным утилитам;
- удаление всех ненужных утилит и системных программ.

Для отслеживания действий отдельных лиц, всем пользователям необходимо присвоить уникальные в рамках компании персональные идентификаторы, идентифицирующие данного пользователя во всех информационных системах.

Для защиты пользователей, которые могут быть мишенью для принуждения, необходимо рассмотреть возможность использования сигнала тревоги, предупреждающего соответствующие службы о принуждении пользователя. Решение о том, использовать ли такой сигнал тревоги или нет, следует принимать исходя из оценки рисков. Для реагирования на сигнал тревоги необходимо определить обязанности и процедуры реагирования.

Для предотвращения доступа незарегистрированных пользователей целесообразно ограничивать время простоя бездействующих терминалов. Средство установления времени простоя должно очищать экран терминала и блокировать сеансы связи с приложениями и сетевыми сервисами после заданного периода бездействия.

Для своевременного выявления попыток несанкционированных действий и принятия, эффективных мер защиты необходимо обеспечить слежение за доступом и использованием информационных систем.

Организация аудита использования информационных систем возлагается на владельцев информационных систем. Непосредственный аудит за безопасным использованием информационных систем возлагается на отдел информационной безопасности.

Руководители структурных подразделений обязаны соблюдать установленные правила и формальные процедуры организации допуска к информационным системам.

11.3.2 Обязанности пользователей

Все сотрудники компании, являющиеся пользователями информационных систем, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности.

11.3.2.1 Требования по использованию паролей

Пользователи должны следовать установленным процедурам поддержания режима безопасности при выборе и использовании паролей. Они обязаны выполнять следующие рекомендации:

- обязательно назначать персональные пароли для обеспечения подотчетности;
- хранить пароли в секрете;
- не записывать пароли на бумаге, если не представляется возможным ее хранение в защищенном месте;
- изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей;
- выбирать пароли, содержащие не менее шести символов;
- при выборе паролей не следует использовать:

• месяцы года, дни недели и т.п.;
• фамилии, инициалы и регистрационные номера автомобилей;
• названия и идентификаторы структурных подразделений;
• номера телефонов или группы символов, состоящие из одних цифр;
• пользовательские идентификаторы и имена, а также идентификаторы групп и другие системные идентификаторы;
• более двух одинаковых символов, следующих друг за другом;
• группы символов, состоящие из одних букв.

- изменять пароли через регулярные промежутки времени (не более чем через 180 суток) и избегать повторное или «циклическое» использование старых паролей;
- чаще изменять пароли для привилегированных системных ресурсов, например, пароли доступа к определенным системным утилитам;
- изменять временные пароли при первом входе в системы;
- не включать пароли в открытые сценарии автоматического входа в системы, например, в макросы или функциональные клавиши.

11.3.2.2 Требования по защите оборудования, оставленного без присмотра

Пользователи обязаны обеспечить надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда оно оставляется без присмотра на продолжительное время. Все пользователи и подрядчики должны знать требования к безопасности и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

При завершении работы с информационной системой пользователи обязаны:

а) завершить активные сеансы связи;

б) выйти из сетевых операционных систем и сетевых сервисов по окончании сеанса связи.

в) защитить ПК или терминалы с помощью блокировки с ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

11.3.2.3 Требования по обеспечению антивирусной защиты

Внедрение комплексной корпоративной системы антивирусной защиты снижает риски потери или утечки информации, сокращает издержки на внедрение и эксплуатацию парка разнородных защитных систем, позволяет предотвратить и устранить последствия вирусной атаки, восстановить работоспособность ИТ-инфраструктуры.

Проникновение в сеть и заражение компьютеров сети вредоносным программным кодом являются сегодня наиболее распространенной угрозой корпоративной безопасности. Путями проникновения компьютерных вирусов, «червей», троянов и т.д. в сеть служат «обычные» в повседневной работе источники – носители информации (CD, DVD, USB и др.), соединения через локальную сеть и интернет, электронная почта.

В общем случае, антивирусная защита информационной системы должна строиться по иерархическому принципу:

−службы общекорпоративного уровня - 1-й уровень иерархии;

−службы подразделений или филиалов - 2-й уровень иерархии;

−службы конечных пользователей - 3-й уровень иерархии.

Службы всех уровней объединяются в единую вычислительную сеть (образуют единую инфраструктуру), посредством локальной вычислительной сети.

Службы общекорпоративного уровня должны функционировать в непрерывном режиме.

Управление всех уровней должно осуществляться специальным персоналом, для чего должны быть предусмотрены средства централизованного администрирования.

Антивирусная система должна предоставлять следующие виды сервисов на общекорпоративном уровне:

– получение обновления программного обеспечения и антивирусных баз;

– управление распространением антивирусного программного обеспечения;

– управление обновлением антивирусных баз;

– контроль за работой системы в целом (получение предупреждений об обнаружении вируса, регулярное получение комплексных отчетов о работе системы в целом);

– на уровне подразделений:

– обновление антивирусных баз конечных пользователей;

– обновление антивирусного программного обеспечения конечных пользователей, управление локальными группами пользователей;

– на уровне конечных пользователей:

– автоматическая антивирусная защита данных пользователя.

Программно-технические компоненты системы антивирусной защиты должны обеспечивать формирование интегрированной вычислительной среды, удовлетворяющей следующим общим принципам создания автоматизированных систем:

– Надежность - система в целом должна обладать продолжать функционировать независимо от функционирования отдельных узлов системы и должна обладать средствами восстановления после отказа.

– Масштабируемость - система антивирусной защиты должна формироваться с учетом роста числа защищенных объектов.

– Открытость - система должна формироваться с учетом возможности пополнения и обновления ее функций и состава, без нарушения функционирования вычислительной среды в целом.

– Совместимость - поддержка антивирусным программным обеспечением максимально-возможного количества сетевых ресурсов. В структуре и функциональных особенностях компонент должны быть представлены средства взаимодействия с другими системами.

– Унифицированность (однородность) - компоненты должны представлять собой стандартные, промышленные системы и средства, имеющие широкую сферу применения и проверенные многократным использованием.

Кроме того, система должна обеспечивать регулярное обновление используемой антивирусной базы, содержать в себе механизмы поиска ранее неизвестных вирусов и макро вирусов, как наиболее распространенных и опасных в настоящее время.

Требования к надежности и функционированию системы

– Система антивирусной защиты не должна нарушать логику работы остальных используемых приложений.

– Система должна обеспечивать возможность вернуться к использованию предыдущей версии антивирусных баз.

– Система должна функционировать в режиме функционирования объекта (рабочая станция/сервер) на котором она установлена.

– Система должна обеспечивать оповещение администратора системы при сбоях или обнаружении вирусов.

Пользователи обязаны следовать установленным процедурам обеспечения антивирусной защиты при вводе информации в систему с внешних магнитных носителей, использовании электронной почты и копировании информации из Интернет.

Категорически запрещается самовольно отключать установленные средства антивирусной защиты и использовать внешние магнитные носители без их предварительной проверки антивирусными средствами.

11.3.3 Администрирование компьютерных систем

Для обеспечения надежного и безопасного функционирования АС должны быть определены обязанности и процедуры по их администрированию.

11.3.3.1 Операционные процедуры и обязанности

Обязанности и процедуры по администрированию и обеспечению функционирования всех компьютеров и сетей должны быть закреплены в должностных инструкциях сотрудников отделов администрирования и информационной безопасности, а также в регламентах использования информационных систем.

Рекомендуется, чтобы выполнение следующих функций не было поручено одним и тем же сотрудникам:

- использование производственных систем;
- ввод данных;
- обеспечение функционирования компьютеров;
- сетевое администрирование;
- системное администрирование;
- разработка и сопровождение систем;
- управление процессом внесения изменений;
- администрирование средств защиты;
- контроль (аудит) средств защиты.

Ответственность за организацию администрирования информационных систем и разработку правил их безопасного использования несут владельцы информационных систем.

Для обеспечения корректной и надежной работы всех функционирующих компьютерных систем должны быть подготовлены ***документированные операционные процедуры***. Документированные процедуры следует также подготавливать для работ, связанных с разработкой, сопровождением и тестированием новых систем.

Процедуры должны включать в себя подробные корректные инструкции по выполнению каждого задания, в том числе (по необходимости) следующие пункты:

а) корректное оперирование с файлами данных;

б) требования к планированию выполнения заданий, включая взаимосвязи с другими системами, а также самое раннее и самое позднее время начала и окончания выполнения заданий;

в) инструкции по обработке ошибок и других исключительных ситуаций, которые могут возникнуть во время выполнения заданий, в том числе ограничения на использование системных утилит;

г) обращение за помощью к персоналу поддержки в случае возникновения технических и других проблем, связанных с эксплуатацией компьютерных систем;

д) процедуры перезапуска и восстановления работоспособности систем, используемые в случае их отказа.

Документированные процедуры должны быть также подготовлены для работ по обслуживанию систем, связанных с администрированием компьютеров и сетей, в том числе процедуры запуска и останова серверов, резервное копирование данных, техническое обслуживание оборудования, управление компьютерными залами и обеспечение их защиты. Операционные процедуры должны рассматриваться как формальные документы, изменения в которые следует

вносить только после их утверждения руководством, наделенным соответствующими полномочиями.

Для обеспечения своевременного, эффективного и организованного реагирования на события, таящие угрозу безопасности, должны быть определены соответствующие управленческие обязанности и процедуры.

Процедуры реагирования на события включают в себя все возможные типы инцидентов в системе безопасности и планирование мер по предотвращению и ослаблению последствий инцидентов в системе безопасности.

11.3.3.2 Защита от вредоносного программного обеспечения

Администраторы АС должны быть всегда готовы к опасности проникновения вредоносного программного обеспечения в системы и по необходимости принимать специальные меры по предотвращению или обнаружению его внедрения.

Необходимо соблюдать следующие рекомендации:

- Использование лицензионного программного обеспечения и запрещение использования несанкционированных программ.
- Противовирусные программные средства следует использовать следующим образом:
  - программные средства обнаружения конкретных вирусов следует применять для проверки компьютеров и носителей информации на наличие известных вирусов либо как мера предосторожности, либо как повседневная процедура;
  - программные средства обнаружения изменений, внесенных в данные, должны быть по необходимости инсталлированы на компьютерах для выявления изменений в выполняемых программах;
- Необходимо проводить регулярную проверку программ и данных в системах, поддерживающих критически важные производственные процессы. Наличие случайных файлов и несанкционированных исправлений должно быть расследовано с помощью формальных процедур.
- Съемные носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.
- Необходимо определить управленческие процедуры и обязанности по уведомлению о случаях поражения систем компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения. Следует составить надлежащие планы обеспечения бесперебойной работы ГАЖК для случаев вирусного заражения, в том числе планы резервного копирования и восстановления всех необходимых данных и программ.

11.3.3.3 Обслуживание систем

Для поддержания целостности и доступности информационных сервисов необходимо определить и использовать повседневные процедуры для снятия резервных копий с данных, процедуры регистрации событий и сбоев, процедуры слежения за средой, в которой функционирует оборудование.

Резервное копирование данных

Резервные копии с критически важных производственных данных и программ должны сниматься регулярно. Для обеспечения возможности восстановления всех критически важных производственных данных и программ после выхода из строя компьютера или отказа носителя информации, необходимо иметь надлежащие средства резервного копирования.

Предлагается соблюдать следующие рекомендации:

- Минимальную дублирующую информацию вместе с точными и полными записями о резервных копиях следует хранить в удаленном месте на достаточном расстоянии для того, чтобы избежать последствий от аварии на основном рабочем месте. Необходимо создать, по крайней мере, три поколения резервных копий данных для важных производственных приложений.
- Резервные копии должны быть надлежащим образом физически защищены от воздействия окружающей среды. Средства защиты носителей информации, принятые на основном рабочем месте, следует распространить на место хранения резервных копий.
- Резервные данные необходимо регулярно тестировать, чтобы быть уверенным, что на них можно будет положиться в случае аварии.

Владельцы данных должны задать период сохранности критически важных производственных данных, а также требования к постоянному хранению архивных копий.

Регистрация сбоев

Необходимо извещать о сбоях в работе систем и предпринимать соответствующие корректирующие меры. Зафиксированные пользователями сбои, касающиеся проблем с компьютерными и коммуникационными системами, следует заносить в журнал регистрации. Должны существовать четкие правила обработки зарегистрированных сбоев, включая следующие:

а) анализ журнала регистрации сбоев для обеспечения их удовлетворительного разрешения;

б) анализ корректирующих мер, цель которого состоит в проверке того, не скомпрометированы ли средства управления безопасностью и является ли предпринятая мера санкционированной.

Слежение за окружающей средой

Для определения условий, которые могут неблагоприятно сказаться на работе компьютерного оборудования и для принятия корректирующих мер, необходимо постоянно следить за окружающей средой, в том числе за влажностью, температурой и качеством источников электропитания. Такие процедуры следует реализовывать в соответствии с рекомендациями поставщиков оборудования.

11.3.3.4 Сетевое администрирование

Управление безопасностью компьютерных сетей, отдельные сегменты которых находятся за пределами ГАЖК, требует особого внимания. Сетевые

администраторы должны определить надлежащие средства контроля для обеспечения защиты данных, циркулирующих в сетях, от несанкционированного доступа. В частности, необходимо рассмотреть следующие пункты:

а) Обязанности по обеспечению работы сетей и компьютеров должны быть по возможности разделены.

б) Необходимо определить обязанности и процедуры по управлению удаленным оборудованием, в том числе оборудованием на рабочих местах пользователей.

в) Для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, целесообразно использование средств криптографической защиты информации и аутентификации сообщений.

г) Необходимо координировать работы по администрированию компьютеров и сетей как для оптимизации сервиса для производственных нужд, так и для обеспечения согласованной реализации защитных мер для всех информационных сервисов.

11.4 Защита технических средств

11.4.1 Защита серверов

Меры по защите серверов могут включать:

Защиту серверов от физического доступа неавторизованного персонала путем:

- размещения серверов в отдельном помещении, доступ в которое ограничен, либо их размещение в закрытых шкафах (стойках), позволяющих исключить доступ к оборудованию и организовать контроль доступа персонала (путем опечатывания, опломбирования, оснащения датчиками вскрытия дверей, подключаемых к системе охранной сигнализации и т.д.);
- контроля физического доступа к серверу.

Защиту от несанкционированного доступа к информации, хранящейся на серверах путем:

- использования доверенных программно-аппаратных средств аутентификации и разграничения доступа;
- регулярной установки обновлений от производителя ОС на сервера;
- удаленное управление сервером должно быть исключено путем соответствующей его настройки.

Защиту от доступа к информации в оперативной памяти серверов путем:

- очистки освобожденной памяти перед выделением ее другим приложениям;
- использования дополнительных средств очистки оперативной памяти.

Защиту от аппаратных вложений или программных закладок путем:

- использования серверов и коммуникационного оборудования, прошедшего проверку на отсутствие специально внедренных электронных устройств;
- использования сертифицированных программных средств.

Защиту от действия вредоносных программ путем:

– использования антивирусных средств;

– контроля целостности программной среды;

– предварительной проверки на отсутствие вирусов при вводе информации с машинных носителей;

– регламента установки нового ПО, включающего в себя процедуру проверки этого ПО;

– установки ПО авторизованными лицами;

– запрета пользователям системы внесения в систему неконтролируемого ПО, в том числе, возможности создания программ на рабочем месте.

– регулярной установки обновлений от производителя ОС на серверах.

Защиту от атак типа «отказ в обслуживании» со стороны сети путем:

– исключения возможности неконтролируемого внесения в информационную систему новых программных модулей, которые могли бы делать попытки соответствующих атак;

– регулярной установки обновлений от производителя ОС на серверах.

Защиту от некомпетентного использования, настройки или неправомерного отключения средств защиты путем:

– размещения серверов в отдельном помещении, доступ в которое ограничен;

– контроля физического доступа к серверу;

– обучения обслуживающего персонала.

Защиту от неправомерного включения, выключения сервера или изменения режимов работы устройств и программ путем:

– размещения серверов в отдельном помещении, доступ в которое ограничен;

– контроля физического доступа к серверу;

– строгой регламентации деятельности обслуживающего персонала по эксплуатации и обслуживанию серверов.

11.4.2 Защита АРМ и рабочих станций пользователей

Меры по защите автоматизированных рабочих мест пользователей могут включать:

Защиту от несанкционированного доступа к компьютерам путем:

– использования электронного замка для обеспечения доверенной загрузки ОС и исключения загрузки с внешнего носителя;

– автоматического блокирования сеанса пользователя при превышении периода неактивности;

– регулярной установки обновлений от производителя ОС.

Защиту от использования незарегистрированных носителей информации путем:

– организационных мер (инструкции и контроль) по обеспечению использования только зарегистрированных носителей. Учет и контроль отчуждаемых носителей информации.

– блокирования интерфейсов ПК, которые могут быть использованы для несанкционированного подключения внешних носителей (LPT, COM, USB, SCSII и

т.п.). Может быть выполнено как физическое блокирование разъемов на корпусе компьютера, так и блокирование за счет применения электронного замка.

Защиту от нелегального внедрения и использования неучтенных программ путем:

– Использования системы защиты информации (СЗИ), обеспечивающей создание замкнутой программной среды на АРМ пользователя, исключающей использование неразрешенного программного обеспечения;

– блокирования интерфейсов ПК, которые могут быть использованы для несанкционированного подключения внешних носителей (LPT, COM, USB, SCSII и т.п.);

– организационных мер, предусматривающих, что установку программного обеспечения на АРМ разрешается производить только администраторам.

Защиту от несанкционированного копирования данных путем:

– блокирования интерфейсов ПК, которые могут быть использованы для несанкционированного подключения внешних носителей (LPT, COM, USB, SCSII и т.п.);

– учета и контроля отчуждаемых носителей информации.

Защиту от доступа к информации, отображаемой на мониторе АРМ путем:

– использования системы контроля и разграничения доступа в рабочие помещения;

– организационных мер (инструкции и контроль) по ограничению доступа посторонних лиц в рабочие помещения компании, в которых установлены АРМ пользователей;

– временной блокировки работы АРМ и гашения монитора при длительной неактивности пользователя или по его команде;

– принятия мер, не позволяющих применять средства удаленного наблюдения (шторы, разворот дисплея и т.п.).

Защиту от действий вредоносных программ, вирусов путем:

– использования сертифицированных антивирусных средств и регулярного обновление баз антивирусов;

– регулярной установки обновлений от производителя ОС на АРМ пользователей.

Защиту от хищения носителей информации путем:

– организационно-технических мер по обеспечению хранения носителей информации: учет носителей, запрет на использование неучтенных носителей, хранение носителей в сейфах.

Защиту от доступа к информации в оперативной памяти компьютера путем:

– использования СЗИ, обеспечивающей создание замкнутой программной среды на АРМ пользователя, исключающей использование неразрешенного программного обеспечения;

– применения механизмов стирания областей оперативной памяти, выделяемых программам, файлам на дисках, файла подкачки страниц по завершении сеанса работы.

Защиту от действия по дезорганизации функционирования системы (в том числе от атаки типа «отказ в обслуживании» со стороны сети) путем:

– регулярной установки обновлений от производителя ОС на АРМ пользователей;

– использования СЗИ, обеспечивающей создание замкнутой программной среды на АРМ пользователя, исключающей использование неразрешенного программного обеспечения;

– использования сертифицированных антивирусных средств и регулярного обновление баз антивирусов;

– исключения из системы средств разработки и отладки программ;

– подбора персонала, исключающего возможность сговора для проведения деструктивных действий;

– ведения контроля действий пользователей средствами защиты информации.

Защиту от умышленной модификации информации путем:

– ведение контроля действий пользователей средствами защиты информации;

– выполнения регламента по резервному копированию критичной информации.

Защиту от проявления ошибок программно-аппаратных средств путем:

– выполнения регламента по резервному копированию информации;

– хранения эталонных версий используемого ПО, периодическое обновление и контроль их работоспособности.

Защиту от некомпетентного использования, настройки или неправомерного отключения средств защиты путем:

– использования средств доверенной загрузки ОС на АРМ пользователя;

– использования СЗИ, обеспечивающей создание замкнутой программной среды на АРМ пользователя, исключающей использование неразрешенного программного обеспечения;

– подбора персонала, исключающего возможность сговора для проведения деструктивных действий. Обучение и переподготовка персонала.

Защиту от ввода ошибочных данных путем:

– организации контроля ввода данных.

11.4.3 Меры по защите коммуникационных средств

Меры по защите коммуникационных средств могут включать:

Защиту от незаконного подключения к линиям связи путем:

– использования СЗИ, обеспечивающей шифрование трафика в каналах связи вне контролируемой зоны;

– физической защиты кабельной системы от доступа посторонних лиц;

– защиты коммутационного оборудования с использованием средств контроля и разграничения доступа.

Защиту от незаконного подключения к сетевому оборудованию путем:

– использования системы контроля доступа в помещения с коммуникационным оборудованием;

– размещения сетевого оборудования в стойках с исключением возможности физического доступа неавторизованного персонала.

Защиту от программного перехвата данных, передаваемых по СКС путем:

– использования СЗИ, обеспечивающей создание замкнутой программной среды на АРМ пользователя, исключающей использование неразрешенного программного обеспечения;

– удаления из системы средств разработки и отладки программ.

Защиту от повреждения СКС путем:

– физической защиты СКС от доступа посторонних лиц.

Защиту от действий, приводящих к некорректному функционированию сетевого оборудования путем:

– контроля за действиями пользователей с целью исключения несанкционированного изменения параметров настройки сетевого оборудования и задействования, возможно имеющихся недекларируемых функций (активации логических каналов утечки информации);

– удаления из системы средств разработки и отладки программ;

– подбора и подготовки обслуживающего персонала.

Защиту от действий, приводящих к частичному или полному отказу сетевого оборудования путем:

– контроля за действиями пользователей;

– использования системы контроля и разграничения доступа в помещения с сетевым оборудованием;

– исключения несанкционированного удаленного управления сетевым оборудованием и использование его встроенных средств защиты от НСД;

– подбора и подготовки обслуживающего персонала.

Защиту от неправомерного включения, выключения оборудования путем:

– использования системы контроля и разграничения доступа в помещения с коммуникационным и серверным оборудованием;

– использования системы контроля доступа в рабочие помещения;

– организационных мер, вынуждающих производить критичные действия только под наблюдением второго лица (правило «двух рук»).

Защиту от неправомерной модификации передаваемых данных, технической и служебной информации путем:

– использования СЗИ для создания замкнутой программной среды на АРМ пользователя, поддерживающей контроль целостности передаваемой информации и исключающей использование неразрешенного программного обеспечения;

– подбора персонала, исключающего возможность сговора для проведения деструктивных действий.

11.5 Работа с носителями информации и их защита

Для защиты компьютерных носителей информации (магнитные ленты, диски, кассеты, флешки, внешние жесткие диски), входных/выходных данных и системной документации от повреждения, похищения и несанкционированного доступа должны быть определены надлежащие операционные процедуры, регламентирующие порядок обращения с ними. Ответственность за установление процедур и правил обращения с носителями информации возлагается на владельцев этих ресурсов.

Все должностные лица и сотрудники компании обязаны неукоснительно выполнять установленные правила и соблюдать рекомендации, предлагаемые ниже.

11.5.1 Управление съемными компьютерными носителями информации

Для управления съемными носителями информации такими, как магнитные ленты, диски, кассеты и распечатки, предлагается использовать следующие меры:

- хранение всех носителей информации осуществлять в надежной, защищенной среде в соответствии с инструкциями производителей;
- использовать систему хранения данных, в которой запрещается использовать описательные метки, т.е. по меткам нельзя определить, какие данные хранятся на запоминающем устройстве;
- использовать стирание предыдущего содержимого повторно используемых носителей информации, которые подлежат удалению, если они больше не нужны;
- получение письменной санкции на утилизацию носителей информации и регистрация всех случаев их утилизации в контрольном журнале.

Все процедуры и уровни полномочий по работе со съемными носителями информации должны быть четко задокументированы.

11.5.2 Процедуры оперирования данными

Чтобы защитить конфиденциальные данные от несанкционированного раскрытия или использования, необходимо определить процедуры оперирования с такими данными. Должны быть подготовлены процедуры для безопасного оперирования со всеми носителями входных и выходных конфиденциальных данных, например, документов, телексов, магнитных лент, дисков, отчетов, незаполненных чеков, счетов и др.

Владельцам данных предлагается разработать рекомендации по следующим пунктам:

а) оперирование с носителями входной и выходной информации и их маркировка;

б) формальная регистрация получателей данных, имеющих соответствующие полномочия;

в) обеспечение полноты входных данных;

г) подтверждение получения переданных данных (по необходимости);

д) предоставление доступа к данным минимальному числу лиц;

е) четкая маркировка всех копий данных для получателя, имеющего соответствующие полномочия;

ж) проверка списков получателей с правом доступа к данным через регулярные промежутки времени.

11.5.3 Защита системной документации

Системная документация может содержать конфиденциальную информацию, например, описание прикладных процессов, процедур, структуры данных и процессов подтверждения полномочий. Для защиты системной документации от несанкционированного доступа, необходимо применять следующие средства контроля:

а) Системная документация должна храниться в надежных шкафах под замком.

Б) Список лиц с правом доступа к системной документации должен быть максимально ограничен, а разрешение на ее использование должно выдаваться руководителем подразделения, хранящего документацию.

11.5.4 Утилизация носителей данных

Для утилизации компьютерных носителей информации, которые больше не нужны, требуются надежные и проверенные процедуры. Конфиденциальная информация может просочиться за пределы ГАЖК и попасть в руки лиц, не имеющих соответствующих прав, вследствие небрежной утилизации компьютерных носителей данных. Для сведения такого риска к минимуму следует определить четкие процедуры уничтожения носителей информации или надежного удаления с них информации. Предлагаются следующие рекомендации:

- Носители данных, содержащих конфиденциальную информацию, необходимо уничтожать, например, посредством их сжигания или измельчения (дробления), или освобождать от данных для использования другими приложениями, но только внутри ГАЖК.
- Для идентификации носителей данных, которые могут потребовать утилизации, предлагается использовать следующий контрольный список:

а) входная документация, например, телексы;
б) копировальная бумага;
в) выходные отчеты;
г) одноразовые ленты для принтеров;
д) магнитные ленты;
е) съемные диски или кассеты;
ж) распечатки программ;
з) тестовые данные;
и) системная документация.

Каждый случай удаления носителей конфиденциальной информации необходимо (по возможности) регистрировать в контрольном журнале для будущих справок.

При накоплении информации, подлежащей удалению, следует учитывать эффект аккумуляции, который может привести к тому, что большое количество

несекретной информации становится более конфиденциальной, чем малое количество конфиденциальной информации.

11.6 Обмен данными и программами

Для предотвращения потери, модификации и несанкционированного использования данных необходимо контролировать обмены данными и программами между подразделениями и клиентами компании. Такие обмены следует осуществлять на основе формальных соглашений.

Для защиты носителей информации во время их транспортировки должны быть установлены процедуры и стандарты, регламентирующие требования к безопасности.

При использовании электронного обмена данными и сообщениями электронной почты необходимо учитывать риски, способные привести к нежелательным последствиям для производственной деятельности компании, и предпринять защитные меры для их ограничения до допустимых пределов.

Соглашения между организациями об обмене (электронном или посредством курьеров) данными и программами должны отражать степень важности производственной информации, участвующей в процессе обмена, и содержать надлежащие условия безопасности, включая следующее:

а) управленческие обязанности по контролю и уведомлению о передаче и получении данных;

б) процедуры уведомления о передаче и получении данных;

в) минимум технических стандартов по упаковке и передаче информации;

г) стандарты по идентификации курьеров;

д) обязанности и обязательства в случае потери данных;

е) права собственности на данные и программы, а также обязанности по защите данных, соблюдении авторских прав на программное обеспечение и т.п.;

ж) технические стандарты на запись и чтение данных и программ;

з) специальные меры, требуемые для защиты особо важных данных, таких, как криптографические ключи.

11.7 Меры по обеспечению физической безопасности оборудования

Информационные системы, поддерживающие критически важные или уязвимые сервисы компании, должны размещаться в защищенных областях, ограниченных определенным периметром безопасности, с надлежащим контролем доступа в помещения и защитными барьерами, и быть физически защищены от несанкционированного доступа, повреждения и помех.

11.7.1 Физический периметр безопасности

Требования к каждому защитному барьеру и его месторасположению должны определяться ценностью ресурсов и сервисов, подлежащих защите, а также

рисками нарушения безопасности и существующими защитными мерами. Каждый уровень физической защиты должен иметь определенный периметр безопасности, в пределах которого обеспечивается надлежащий уровень защиты.

При организации периметра безопасности предлагается соблюдать следующие рекомендации:

а) Периметр безопасности должен соответствовать ценности защищаемых ресурсов и сервисов.

б) Периметр безопасности должен быть четко определен.

в) Вспомогательное оборудование (например, фотокопировальные аппараты, факс-машины) должны быть размещены так, чтобы уменьшить риск несанкционированного доступа к защищенным областям или компрометации конфиденциальной информации.

г) Физические барьеры должны по необходимости простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение и загрязнение окружающей среды.

д) Не следует предоставлять посторонним лицам информацию о том, что делается в защищенных областях без надобности.

е) Компьютерное оборудование, принадлежащее ГАЖК, следует размещать в специально предназначенных для этого местах, отдельно от оборудования, контролируемого сторонними организациями.

ж) В нерабочее время защищенные области должны быть физически недоступны (закрыты на замки) и периодически проверяться охраной.

з) Персоналу, осуществляющему техническое обслуживание сервисов, должен быть предоставлен доступ в защищенные области только в случае необходимости, и после получения разрешения. Доступ такого персонала (особенно к конфиденциальным данным) следует ограничить, а их действия следует отслеживать.

и) В пределах периметра безопасности использование фотографической, звукозаписывающей и видео аппаратуры должно быть запрещено, за исключением санкционированных случаев.

11.7.2 Типовые требования к оборудованию помещений

Защищаемые помещения должны находиться внутри периметров безопасности и оборудоваться системами охранно-пожарной сигнализации, механическими или электрическими замками на двери и иметь, если они расположены в нижних этажах зданий, металлические решетки на окнах.

При необходимости повышенного уровня защиты могут использоваться системы видеонаблюдения и автоматического пожаротушения.

При выходе сотрудников из защищаемых помещений они обязаны закрывать их на ключ. В нерабочее время защищаемые помещения должны сдаваться под охрану.

11.7.3 Контроль доступа в помещения

В защищенных областях следует установить надлежащий контроль доступа в помещения, чтобы только персонал, имеющий соответствующие полномочия, имел к ним доступ. Предлагается рассмотреть следующие средства контроля:

а) За посетителями защищенных областей необходимо установить надзор, а дата и время их входа и выхода должны регистрироваться. Посетителям должен быть предоставлен доступ для конкретных, разрешенных целей.

б) Весь персонал, работающий в защищенных областях, должен носить на одежде хорошо различимые идентификационные карточки; кроме того, следует рекомендовать им спрашивать пропуск у незнакомых лиц.

в) Необходимо немедленно изъять права доступа в защищенные области у сотрудников, увольняющихся с данного места работы.

11.7.4 Размещение и защита оборудования

Для предотвращения потери, повреждения и компрометации ресурсов, необходимо обеспечить физическую защиту оборудования от угроз нарушения безопасности и опасностей, представляемых окружающей средой.

Предлагается соблюдать следующие рекомендации:

а) Оборудование следует размещать так, чтобы по возможности свести к минимуму излишний доступ в рабочие помещения. Рабочие станции, поддерживающие конфиденциальные данные, должны быть расположены так, чтобы они были всегда на виду.

б) Следует рассмотреть возможность изоляции областей, требующих специальной защиты, чтобы понизить необходимый уровень общей защиты.

в) Для идентификации возможных опасностей предлагается использовать следующий контрольный список:

- пожар;
- задымление;
- затопление;
- запыление;
- вибрация;
- влияние химических веществ;
- помехи в электропитании;
- электромагнитное излучение.

г) Следует запретить прием пищи и курение в местах размещения компьютерного оборудования.

Следует рассмотреть возможные опасности, как на данном этаже, так и на соседних этажах.

11.7.5 Источники электропитания

Оборудование необходимо защищать от сбоев в системе электропитании и других неполадок в электрической сети. Источник питания должен соответствовать спецификациям производителя оборудования.

Следует рассмотреть необходимость использования резервного источника питания. Для оборудования, поддерживающего критически важные производственные сервисы, рекомендуется установить источник бесперебойного питания. План действий в чрезвычайных ситуациях должен включать меры, которые необходимо принять по окончании срока годности источников бесперебойного питания. Оборудование, работающее с источниками бесперебойного питания, необходимо регулярно тестировать в соответствии с рекомендациями изготовителя.

11.7.6 Техническое обслуживание оборудования

Необходимо осуществлять надлежащее техническое обслуживание оборудования, чтобы обеспечить его постоянную доступность и целостность. Предлагаются следующие рекомендации:

а) Техническое обслуживание оборудования должно осуществляться через промежутки времени, рекомендуемые поставщиком, и в соответствии с инструкциями.

б) Ремонт и обслуживание оборудования должен выполнять только персонал поддержки, имеющий соответствующие полномочия.

в) Необходимо регистрировать все неисправности и неполадки.

11.7.7 Защита кабельной разводки

Кабели электропитания и сетевые кабели для передачи данных необходимо защищать от вскрытия для целей перехвата информации и повреждения. Для уменьшения такого риска в помещениях компании предлагается реализовать следующие защитные меры:

а) Кабели электропитания и линии связи, идущие к информационным системам, должны быть проведены (по возможности) под землей или защищены надлежащим образом с помощью других средств.

б) Необходимо рассмотреть меры по защите сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, например, воспользовавшись экранами или проложив эти линии так, чтобы они не проходили через общедоступные места.

в) Незадействованные разъемы информационных кабелей, предназначенные для подключения рабочих станций, должны быть опечатаны или заклеены специальной маркой для исключения возможности несанкционированного подключения нештатных технических средств обработки информации.

Для исключительно уязвимых или критически важных систем следует рассмотреть необходимость принятия дополнительных мер, таких, как:

- шифрование данных;
- установку бронированных экранов и использование запираемых помещений;
- использование других маршрутов или сред передачи данных.

11.7.8 Защита оборудования, используемого за пределами компании

Использование оборудования информационных систем (независимо от того, кто им владеет), поддерживающих производственные процессы за пределами компании, должно быть санкционировано руководством. Уровень защиты такого оборудования должен быть таким же, как и для оборудования, расположенного на территории компании. Предлагается соблюдать следующие рекомендации:

а) Сотрудникам запрещается использовать персональные компьютеры для продолжения работы на дому, если не установлена процедура проверки на наличие вирусов.

б) Во время поездок запрещается оставлять оборудование и носители информации в общедоступных местах без присмотра. Портативные компьютеры следует провозить в качестве ручного багажа.

в) Во время поездок портативные компьютеры уязвимы по отношению к кражам, потери и несанкционированного доступа. Для таких компьютеров следует обеспечить надлежащую защиту доступа, чтобы предотвратить несанкционированный доступ к хранящейся в них информации.

г) Следует всегда соблюдать инструкции производителя, касающиеся защиты оборудования, например, защищать оборудование от воздействия сильных электромагнитных полей.

Риски нарушения безопасности (например, повреждения, кражи, перехвата), могут значительно варьировать от места к месту; это следует обязательно учитывать при определении наиболее подходящих защитных средств.

11.7.9 Надежная утилизация оборудования

Данные ГАЖК могут быть скомпрометированы вследствие небрежной утилизации оборудования. Перед утилизацией оборудования все его компоненты, включая носители информации, например жесткие диски, необходимо проверять, чтобы гарантировать, что конфиденциальные данные и лицензированное программное обеспечение было удалено. Поврежденные запоминающие устройства, содержащие особо ценные данные, могут потребовать оценки рисков для того, чтобы определить, следует ли их уничтожать, ремонтировать или избавиться от них.

11.8 Меры по безопасности при разработке и сопровождении информационных систем

11.8.1 Анализ и задание требований по безопасности при проектировании информационных систем

При проектировании информационных систем необходимо задать требования по обеспечению их безопасного использования и защиты от НСД обрабатываемой в них информации. В технических заданиях необходимо определить:

- категории важности обрабатываемой информации, цели и необходимые средства ее защиты, требования по эффективности безопасного использования системы.

- требования к средствам резервирования, дублирования, регистрации событий, контроля целостности, контроля завершения процессов, возможностей откатов, возможностей восстановления после сбоев и т.д.
- ограничения по использованию протоколов взаимодействия, программных и аппаратных средств и, в том числе, средств защиты.
- предъявляемые к персоналу ИС, и методам контроля безопасного использования системы.
- перечень и содержание документов, необходимых для безопасного использования и обслуживания системы.

11.8.2 Меры по безопасности в прикладных системах

При работе с прикладными системами сотрудники компании обязаны соблюдать меры безопасности, установленные владельцами этих систем.

Владельцы прикладных систем и производственных приложений обязаны сформировать требования (инструкции) к переходу систем на аварийный режим исходя из процесса планирования бесперебойной работы . Поставщики услуг должны согласовать требования к переходу на аварийный режим для коллективно используемых сервисов и составить соответствующий план перехода на него для каждого из них.

Для повышения надежности критичных систем и временного продолжения обработки данных в случае повреждения или отказа основного оборудования должно быть предусмотрено аварийное резервное оборудование. Администраторы сетей обязаны заблаговременно подготовить соответствующий план перехода на аварийный режим для каждого информационного сервиса.

Аварийное резервное оборудование, планы и процедуры перехода на аварийный режим необходимо регулярно тестировать.

11.8.3 Меры по безопасности при приемке и внедрении новых систем

11.8.3.1 Планирование систем и их приемка

Для обеспечения доступности ресурсов и надлежащей нагрузочной способности систем, требуется заблаговременное планирование и подготовка.

Чтобы уменьшить риск перегрузки систем, необходимо на основе прогноза оценить будущие потребности в их нагрузочной способности. Эксплуатационные требования к новым системам следует определить, задокументировать и проверить до их приемки. Требования к переходу на аварийный режим для сервисов, поддерживающих многочисленные приложения, должны быть согласованы, и регулярно пересматриваться.

11.8.3.2 Планирование нагрузки

Для того чтобы избежать отказов систем вследствие их недостаточной нагрузочной способности, необходимо постоянно следить за их нагрузкой. Для обеспечения надлежащей производительности компьютеров и емкости запоминающих устройств, следует оценить будущие потребности в их нагрузочной способности на основе прогноза. Этот прогноз должен учитывать требования к

новым системам, а также текущие и прогнозируемые тенденции использования компьютеров и сетей.

Администраторы компьютеров и сетей должны использовать эту информацию для выявления возможных «узких мест», которые могут представлять угрозу системе безопасности или пользовательским сервисам, и планирования надлежащих мер по исправлению ситуации.

11.8.3.3 Приемка систем

Приемка систем осуществляется специальной комиссией ГАЖК. Персональный состав комиссии, цели и сроки проведения приемки систем определяются в приказе.

Приёмочные испытания целесообразно проводить в соответствии с рекомендациями ГОСТ 34.601-90 "Автоматизированные системы. Стадии создания". Процесс приемки систем включает:

а) проведение испытаний на соответствие техническому заданию в соответствии с программой и методикой приёмочных испытаний;

б) анализ результатов испытания системы и устранение недостатков, выявленных при испытаниях;

в) оформление акта о приёмке системы в постоянную эксплуатацию.

При приемке новых систем администраторы систем должны проверить следующие пункты:

а) требования к производительности и нагрузочной способности компьютеров;

б) подготовку процедур восстановления и перезапуска систем после сбоев, а также планов действий в экстремальных ситуациях;

в) подготовку и тестирование повседневных операционных процедур в соответствии с заданными стандартами;

г) проверку, что установка новой системы не будет иметь пагубных последствий для функционирующих систем, особенно в моменты пиковой нагрузки на процессоры;

д) подготовку персонала к использованию новых систем.

Для определения реальных потребительских качеств системы и выявления скрытых недостатков перед проведением приемочных испытаний целесообразно осуществлять проведение предварительных испытаний и опытную эксплуатацию системы в течение двух – трех месяцев.

11.8.4 Меры по безопасности в среде разработки и рабочей среде

Работы, связанные с разработкой и тестированием систем, могут привести к непреднамеренному внесению изменений в программы и данные, совместно используемые в одной и той же вычислительной среде. Поэтому целесообразно провести разделение программных средств разработки и рабочих программ для уменьшения риска случайного внесения изменений или несанкционированного доступа к рабочему программному обеспечению и производственным данным. Предлагаются следующие средства контроля:

а) Программные средства разработки и рабочие программы должны по возможности запускаться на разных серверах или в разных директориях/сегментах сети.

б) Компиляторы, редакторы и другие системные утилиты не должны храниться вместе с рабочими системами, если в этом нет необходимости.

в) Для уменьшения риска путаницы, следует использовать разные процедуры входа в рабочие и тестируемые системы. Необходимо обеспечить использование разных паролей для входа в эти системы, а система меню должна выводить на экран соответствующие идентификационные сообщения.

Необходимо контролировать внесение изменений в информационные системы. Следует определить формальные управленческие процедуры и обязанности для обеспечения удовлетворительного контроля за внесением всех изменений в оборудование, программы и процедуры. В частности, необходимо рассмотреть следующие пункты:

а) выявление и регистрация существенных изменений;

б) оценка возможных последствий от таких изменений;

в) процедура утверждения предлагаемых изменений;

г) доведение деталей предлагаемых изменений до сведения всех лиц, которых они могут затронуть;

д) процедуры и обязанности по ликвидации неудачных изменений и восстановлению систем после их внесения.

12 КОНТРОЛЬ ЭФФЕКТИВНОСТИ ПРИНИМАЕМЫХ МЕР ЗАЩИТЫ

Для поддержания требуемого уровня информационной безопасности в ГАЖК необходимо осуществлять постоянный контроль эффективности принимаемых мер защиты. Основным критерием при этом является то, что риски защищаемым ресурсам находятся в диапазонах, приемлемых для компании.

Ответственность за контроль эффективности принимаемых мер защиты несут владельцы защищаемых ресурсов и должностные лица инфраструктуры информационной безопасности.

Планирование и непосредственное осуществление контроля состояния информационной безопасности в компании возлагается на отдел информационной безопасности.

Основными механизмами контроля эффективности принимаемых мер защиты являются – мониторинг и аудит информационной безопасности.

12.1 Мониторинг информационной безопасности ГАЖК

Для постоянного контроля требований принятой политики информационной безопасности, своевременного обнаружения и регистрации отклонений, защитных мер от требований ИБ, персоналом компании ответственным за информационную безопасность должен проводиться мониторинг информационной безопасности.

Мониторинг информационной безопасности (стандарты O’z DSt ISO/IEC 27001, O’z DSt ISO/IEC 15408, ISO 17799) должен осуществляться по двум основным направлениям:

- мониторинг событий нарушения ИБ, поступающих от средств защиты (сетевые атаки, обнаружение вирусов, регистрация попыток НСД и т.д.). Этот вид мониторинга позволяет реагировать и блокировать атаки сразу же по их обнаружению и за счет этого предотвращать или снижать возможный ущерб от их реализации;
- мониторинг нарушения сотрудниками компании установленных требований политики информационной безопасности. Этот вид мониторинга позволяет выявлять нарушения до проявления угрозы и принять соответствующие превентивные меры.

Основными целями мониторинга ИБ являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных для осуществления:

- контроля за реализацией требований политики информационной безопасности;
- контроля за реализацией положений государственных нормативных актов по обеспечению ИБ;
- выявления нештатных (или злоумышленных) действий в АС;
- выявления потенциальных нарушений ИБ;
- своевременного выявления и блокирования угроз.

Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные программные средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

12.2 Аудит информационной безопасности ГАЖК

Деятельность, относящаяся к обеспечению ИБ, должна контролироваться.

По определению - аудит информационной безопасности организации - это систематический, независимый и документируемый процесс получения свидетельств аудита ИБ и объективного их оценивания с целью установления степени выполнения в организации установленных критериев аудита ИБ.

Аудит может проводиться самой ГАЖК и внешними организациями.

Внутренние аудиты («аудиты первой стороной») проводятся самой компанией или от его имени для анализа менеджмента или других внутренних целей и могут служить основанием для самодекларации ГАЖК о соответствии требованиям по ИБ. Порядок и периодичность проведения внутреннего аудита ИБ ГАЖК в целом (или отдельных структурных подразделений) определяется руководством. Для проведения внутреннего аудита создается рабочая комиссия из сотрудников ЦА ГАЖК и структурных подразделений .

Внешние аудиты включают «аудиты второй стороной» и «аудиты третьей стороной». Аудиты второй стороной проводятся сторонами, заинтересованными в деятельности компании, например, потребителями или другими лицами от их имени. Аудиты третьей стороной проводятся внешними независимыми организациями на договорной основе в соответствии с действующим законодательством. В качестве третьей стороны выступающей внешним аудитором ИБ создана Служба реагирования на компьютерные инциденты (UZ-CERT) при UZINFOCOM в соответствии с Постановлением Президента Республики

Узбекистан №167 «О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем» от 5 сентября 2005 года. При проведении внешнего аудита ИБ руководство организации должно обеспечить документальное и, если это необходимо, техническое подтверждение того, что:

- политика ИБ отражает требования бизнеса и цели организации;
- организационная структура управления ИБ создана;
- процессы выполнения требований ИБ исполняются и удовлетворяют поставленным целям;
- защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;
- остаточные риски оценены и остаются приемлемыми для организации;
- система управления ИБ соответствует определенному уровню зрелости управления ИБ;
- рекомендации предшествующих аудитов ИБ реализованы.

Основными методами получения свидетельств аудита ИБ являются:

- проверка документов, касающихся обеспечения ИБ и отражающих принципы, положения и требования стандартов;
- проверка (с помощью наблюдения) выполнения сотрудниками проверяемой организации существующих политик ИБ организации;
- устный опрос сотрудников проверяемой организации и независимой (третьей) стороны.

Оценка соответствия ИБ принципам, положениям и требованиям стандарта осуществляется на основе документа «Методика оценки соответствия информационной безопасности», которая определяет:

- направления оценки соответствия ИБ– оценка текущего уровня ИБ, оценка тенденции в обеспечении ИБ, оценка осознания значения ИБ;
- показатели ИБ, отражающие принципы, положения и требования стандарта;
- способы формирования и отображения итоговой оценки соответствия ИБ.

В соответствии с результатами аудита информационной безопасности формируется рейтинг ГАЖК в обеспечении ИБ. Этот рейтинг формируется из совокупности трех оценок:

- осознание значения ИБ для деятельности (достижения целей бизнеса) организации;
- тенденция в обеспечении ИБ;
- текущий уровень ИБ.

Оценка по каждому из направлений вычисляется как среднее арифметическое соответствующих групповых показателей ИБ, перечисленных в методике.

Полученный в результате проведения оценки соответствия ИБ стандарту рейтинг является основой для формирования аудиторского заключения. Оно может быть:

- безусловно положительное;
- условно положительное;
- отрицательное;

- отказ от выражения заключения.

Аудиторский отчет должен храниться в Специальной службе ГАЖК в течение установленного времени. Доступ к аудиторскому отчету должен быть разрешен только руководству ГАЖК и руководителям отделов информационной безопасности.

13. ПОРЯДОК УТВЕРЖДЕНИЯ, ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

Настоящая Политика вступает в законную силу с даты утверждения руководством ГАЖК. Требования настоящей Политики могут развиваться другим внутренними нормативными документами ГАЖК, которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов, а также Устава ГАЖК настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу ГАЖК. В этом случае Управление обеспечения информационной безопасности и информационного развития обязано незамедлительно инициировать внесение соответствующих изменений.

Изменения и дополнения в настоящую Политику вносятся по инициативе структурных подразделений компании, согласовав с Управлением обеспечения информационной безопасности и информационного развития, и утверждаются решением руководством ГАЖК.

Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;
- внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

Ответственным за внесение изменений в настоящую Политику является начальник Управления обеспечения информационной безопасности и информационного развития.

Настоящая Политика информационной безопасности ГАЖК «Узбекистон темир йуллари» не заменяет действующие стандарты, руководящие документы и инструкции.

Приводимые руководства, правила, требования и рекомендации предполагают, что их реализация будет поручена лицам, имеющим надлежащую квалификацию и опыт работы.