Приложение № 10
к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на 2013-2020 годы
от 23 февраля 2016 года № 7

Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан

I. Общие положения

1.1. Настоящие Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан» устанавливают основные принципы и порядок разработки и внедрения политики информационной безопасности в органах государственного и хозяйственного управления, а также органах государственной власти на местах (далее-организации).

1.2. Методическое пособие является основой для выбора практических мероприятий по управлению безопасностью в организации, а также при обеспечении целостности, доступности и конфиденциальности информации при обмене ею между организациями.

1.3. В настоящем Методическом пособии используются термины и определения, согласно O‘zDSt 1047:2003 [1], O‘zDSt 2927:2015 [2], O‘zDSt ISO/IEC 27000:2014 [5].

II. Разработка политики информационной безопасности организации

2.1. Политика информационной безопасности организации

Политика информационной безопасности организации (далее - политика) представляет собой совокупность документированных руководящих принципов, правил, процедур и практических приемов в области информационной безопасности, которыми организация руководствуется в своей деятельности.

2.2. Цели и задачи политики

Целями разработки и внедрения политики являются:

- определение основных информационных систем и ресурсов, подлежащих защите;
- формирование организационно-методической базы для реализации системы управления информационной безопасностью (далее СУИБ).

Основными задачами, решаемыми при разработке политики, являются:

- защита информационных активов от угроз, исходящих от противоправных действий злоумышленников;
- управление непрерывной работой системы:
- уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и

хранения информации, обеспечение нормального функционирования технологических процессов;

- обеспечение информационной безопасности информационных ресурсов и систем, а также персонала организации

- разработка модели нарушителя информационной безопасности организации;

- разработка перечня потенциальных угроз информационной безопасности организации и их анализ;

- классификация информационных ресурсов объекта и их контроль;

- формирование требований к СУИБ;

- определение обязанностей персонала по обеспечению информационной безопасности.

2.3. Порядок разработки политики

Для разработки политики приказом руководителя организации утверждается Рабочая группа, в составе которой обязательно должны быть следующие лица:

представитель руководства организации;

ответственный по вопросам информационной безопасности,

начальник отдела кадров (кадровой службы);

представитель технического персонала (администратор информационной безопасности, администратор сети, администратор баз данных, либо другой компетентный персонал (сотрудник)).

При необходимости, возможно привлечение других сотрудников организации, сторонних профильных организаций или специалистов.

Порядок разработки политики разделяется на следующие этапы:

Первый этап.

Первоначальный аудит безопасности, в том числе проведение предварительного обследования и инвентаризация состояния информационной безопасности, идентификация угроз безопасности организации; идентификация ресурсов, нуждающихся в защите; определение рисков.

В процессе аудита производится анализ текущего состояния ИБ, выявляются существующие уязвимости, наиболее критичные области функционирования и самые чувствительные к угрозам безопасности процессы деятельности организации.

Проведение аудита позволит определить угрозы и уязвимости информационной безопасности организации, получить исходные данные для разработки политики, а также подготовить организацию к дальнейшей аттестации объектов информатизации.

В ходе аудита организации осуществляется следующее:

- изучение и анализ выполнения организацией требований законодательства Республики Узбекистан, указов и постановлений Президента Республики Узбекистан и Кабинета Министров Республики Узбекистан, привести в соответствие с категориями нормативно-правовых актов Республики Узбекистан, а также исполнение нормативных документов, регулирующих вопросы обеспечения информационной безопасности в организации;

- первичное обследование компьютеров и серверов организации, т.е. анализируются настройки используемых операционных систем, прикладного и системного программного обеспечения (ПО), средств защиты информации, а также других аппаратных средств, входящих в информационно-коммуникационные технологии и др.;

- анализ веб-сайта организации на предмет наличия угроз и уязвимостей информационной безопасности;

- анализ внедренных мер обеспечения физической защиты территории, периметра и помещений организации, т.е. анализ системы охраны, средств разграничения доступа, системы пожарной безопасности и др.;

- оценка осведомленности персонала организации установленным в организации правилам информационной безопасности, путём интервьюирования;

- анализ категорирования и инвентаризации информационных и материальных ресурсов организации.

Второй этап.

Разработка проекта политики информационной безопасности организации.

При разработке политики необходимо придерживаться следующих основных правил:

- политика должна полностью подчиняться действующему законодательству и требованиям государственных стандартов;

- текст политики должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования.

В целом политика должна давать ясное представление о требуемом поведении пользователей, администраторов и других специалистов при внедрении и использовании информационных систем и средств защиты информации, а также при осуществлении обмена информацией и выполнении операций по обработке информации.

Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам организации.

Третий этап.

Согласование и введение в действие политики информационной безопасности организации.

Разработанный проект политики в установленном порядке направляется на согласование в Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан и уполномоченным органам и после согласования, вводится в действие приказом руководителя организации. При этом для полноценного введения в действие утвержденной политики необходимо разработать сетевой план мероприятий по внедрению политики с указанием конкретных дат и исполнителей.

В должностные инструкции персонала, положения о подразделениях, договорные (контрактные) обязательства организации должны быть включены обязанности и ответственность по обеспечению информационной безопасности.

Необходимо предусмотреть порядок ознакомления всего персонала организации с требованиями и правилами утвержденной политики, а также проведение регулярных разъяснительных мероприятий по вопросам обеспечения информационной безопасности.

Если требования политики распространяются за пределы организации, в договорные обязательства со сторонними организациями необходимо включать требования информационной безопасности.

2.4. Пересмотр и актуализация политики информационной безопасности организации

Пересмотр политики необходимо осуществлять не реже 1 раза в год, а также в следующих случаях:

- при изменении и утверждении новых нормативно-правовых актов и нормативных документов по информационной безопасности;

- при изменении конфигурации, добавлении или удалении программных и аппаратных, программно-аппаратных средств, не изменяющих технологию информационных процессов;

- при изменении конфигурации и настроек технических средств защиты информации объекта;

- при изменении состава и обязанностей должностных лиц – пользователей и обслуживающего персонала объекта, отвечающих за ее информационную безопасность.

Политика подлежит полному пересмотру в случае изменения технологии информационных процессов или использования новых средств защиты информации.

Проводимые мероприятия по информационной безопасности организации следует регулярно проверять на соответствие принятой политике.

Актуализация и оценка эффективности политики осуществляется путем проведения внутреннего и внешнего аудита информационной инфраструктуры организации на предмет соответствия требованиям и положениям утвержденной политики.

Регулярность проведения аудита определяется политикой, при этом внутренний аудит должен проводиться не реже 1 раза в полгода, а внешний аудит- не реже 1 раза в год.

III. Порядок оформления политики информационной безопасности

3.1. Структура политики информационной безопасности

Структура политики и ее детализация могут отличаться, в зависимости от особенностей организации, но они должны основываться на типовой структуре, включающей следующие разделы:

1. Введение
2. Нормативные ссылки
3. Термины и определения
4. Обозначения и сокращения
5. Область применения
6. Цели и задачи
7. Основные положения
8. Объекты защиты
9. Риск и модель угроз информационной безопасности
10. Модель нарушителя информационной безопасности
11. Меры информационной безопасности
12. Реагирование на инциденты информационной безопасности
13. Обеспечение безопасности каналов связи
14. Распределение ответственности
15. Порядок пересмотра и актуализации политики

Кроме того, политика может включать или содержать ссылки на следующие документы, утверждаемые в установленном порядке руководством организации:

1. Положение о локальной (корпоративной) сети и по организации защищенных сетевых соединений;

2. Положение об обеспечении информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование;

3. Инструкция системного администратора локальной (корпоративной) сети;

4. Положение об отделе обеспечения информационной безопасности (Инструкция администратора информационной безопасности) локальной (корпоративной) сети;

5. Положение по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных;

6. Инструкция по парольной защите;

7. Инструкция по антивирусной защите;

8. Инструкция по обеспечению безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных;

9. Правила по разработке матрицы доступа к информационным ресурсам автоматизированной системы;

10. Перечень разрешенного к использованию программного обеспечения;

11. Инструкция по работе с сетью Интернет и корпоративной электронной почтой;

12. Порядок управления информационными активами организации;

13. Инструкция по организации технической защиты информации;

14. Инструкция по организации криптографической защиты информации;

15. Порядок обращения с информацией, подлежащей защите;

16. План обеспечения непрерывной работы и восстановления работоспособности организации в чрезвычайных (нештатных) ситуациях.

3.2. Содержание разделов политики

1. Введение должно включать в себя общие сведения об организации.

2. Раздел **«Нормативные ссылки»** должен содержать перечень всех нормативных документов, на которые приведены ссылки в политике.

3. В раздел **«Термины и определения»** необходимо включить все используемые в политике термины и определения.

4. В раздел **«Обозначения и сокращения»** необходимо включить все используемые в политике обозначения и сокращения.

5. В разделе **«Область применения»** необходимо указать сферу распространения документа и границы его действия.

6. В разделе **«Цели и задачи»** необходимо привести основные цели и задачи политики.

7. В разделе **«Основные положения»** необходимо отобразить принципы, методы и меры обеспечения информационной безопасности в организации.

8. В разделе **«Объекты защиты»** необходимо отобразить защищаемые активы организации. К активам организации можно отнести следующие:

- персонал организации, информационные ресурсы, чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности, в том числе, общедоступная информация, представленная в виде документов и массивов информации, независимо от формы и вида их представления;

- программные ресурсы – операционные системы и прикладное ПО, средства разработки и утилиты, серверные приложения и сервисы;

- физические ресурсы – компьютерное и коммуникационное оборудование, носители данных, помещения и пр.

9. В разделе **«Риск и модель угроз информационной безопасности»** необходимо привести основные принципы анализа рисков информационной безопасности в организации связанные, в том числе, с взаимодействием со сторонними организациями.

Если доступ сторонних организаций к информационным активам организации и средствам обработки информации необходим по производственным причинам, а также, в случае получения товаров и услуг от сторонних организаций, следует проводить анализ рисков для определения возможных последствий для безопасности информации и требований к средствам управления.

Такие мероприятия следует согласовывать и определять в договорах со сторонней организацией.

9.1. Риски информационной безопасности организации.

Следует определить риски по отношению к информации и средствам ее обработки, принадлежащим организации, со стороны деятельности организации, в которых участвуют стороны, перед предоставлением доступа следует внедрить приемлемые средства управления.

Если есть необходимость в разрешении доступа сторонних организаций к средствам обработки информации и/или информационным активам организации, то для установления требований к конкретным средствам управления следует определить риски. При определении рисков, относящихся к доступу сторонних организаций, следует принимать во внимание:

- средства обработки информации, к которым требуется доступ сторонней организации;

- тип доступа сторонней организации к информации и средствам ее обработки, например:

- физический доступ - к офисным помещениям, компьютерным комнатам, серверным;

- логический доступ - к базам данных и информационным системам организации;

- сетевое соединение между сетями организации и сторонней организацией - постоянное соединение или удаленный доступ.

- предоставляется ли доступ на месте эксплуатации или вне его;

- ценность и конфиденциальность задействованной информации, а также ее чувствительность для организации;

- средства управления, необходимые для защиты информационных активов организации и не предназначенные для предоставления доступа сторонним организациям;

- персонал стороннего субподрядчика, участвующий в обработке информации организации;

- способ идентификации организации или персонала, уполномоченных получать доступ, способ проверки полномочий, а также частоту подтверждения потребности;

- различные способы и средства управления, используемые сторонними организациями для хранения, обработки, передачи, совместного использования и обмена информацией;

- влияние отказа в необходимом доступе к информации на стороннего субподрядчика, а также ввода и получение им неточной или вводящей в заблуждение информации;

- практики и процедуры, связанные с инцидентами информационной безопасности и потенциальными убытками, сроки и условия продолжения доступа сторонней организации в случае инцидента информационной безопасности;

- юридические и нормативные требования, а также другие договорные обязательства, относящиеся к сторонней организации, которые следует принимать во внимание;

- влияние соглашений на интересы любых других заинтересованных сторон.

Организации могут быть подвержены рискам, связанным с внутренними процессами управления коммуникациями организации, если применяется высокая степень аутсорсинга, либо если задействованы несколько сторонних организаций.

Средства управления описывают соглашения с различными сторонними организациями, включая, например:

- поставщиков услуг, таких как провайдеры сети Интернет, телефонные службы, эксплуатационные службы и службы поддержки;

- управляемые службы безопасности;

- аутсорсинг средств и/или операций, например, системы информационных технологий, сервисы накопления информации, центры обработки звонков;

- персонал, осуществляющий поддержку и сопровождение аппаратных средств и программного обеспечения;

- персонал, осуществляющий уборку, охрану, обеспечивающий общественное питание и другие хозяйственные службы;

- временный персонал, студенты и лица, работающие по трудовым соглашениям (клиенты).

Данные соглашения могут помочь снизить риски, связанные со сторонними организациями.

9.2. Угрозы информационной безопасности.

Потенциальные угрозы информационной безопасности по природе их возникновения разделяются на два типа: естественные (объективные) и искусственные (субъективные).

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

Существуют следующие виды угроз информационной безопасности:

1) угрозы нарушения конфиденциальности: хищение (утечка, перехват, съем), утрата (неумышленная потеря), разглашение информации как умышленное, так и неумышленное;

2) угрозы нарушения целостности информации: модификация (искажение) информации, отрицание подлинности информации, навязывание ложной информации;

3) угрозы нарушения доступности информации: блокирование информации, уничтожение информации и средств её обработки и хранения.

В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Источники угроз могут находиться как внутри объекта информатизации - внутренние, так и вне его - внешние.

Все источники угроз делятся на классы, обусловленные типом носителя угрозы (источника угрозы):

- источники угроз, обусловленные действиями субъекта (человеческий фактор), которые могут быть квалифицированы как умышленные или случайные проступки;

- техногенные источники угроз, обусловленные техническими средствами и определяемые технократической деятельностью человека;

- стихийные источники угроз, обусловленные природными явлениями, которые невозможно предусмотреть или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей.

10. В разделе **«Нарушители информационной безопасности»** приводится классификация нарушителей безопасности информации.

Нарушители информационной безопасности по своей принадлежности разделяются на две группы: внутренние и внешние.

Под внутренними потенциальными нарушителями подразумеваться персонал организации, имеющие санкционированный доступ на территорию объектов информатизации.

Под внешними потенциальными нарушителями подразумеваются все остальные лица.

11. В разделе **«Меры информационной безопасности»** необходимо указать, какие меры применяются в части организации процесса обеспечения информационной безопасности, а также процесса соблюдения и выполнения принципов и требований политики.

Основные меры обеспечения информационной безопасности организации подразделяются на:

- правовые меры;
- морально-этические меры;
- организационные меры;
- технологические меры;
- инженерно-технические меры;
- программно-аппаратные меры;
- меры безопасности в отношениях с внешними пользователями.

К правовым мерам информационной безопасности относятся законы Республики Узбекистан, и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в коллективе организации. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или в целом организации. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе организации.

Организационные меры в основном ориентированы на работу с персоналом, выбор местоположения и размещения объектов защиты, организацию систем физической, противопожарной защиты, контроля выполнения принятых мер, возложения персональной ответственности за выполнение мер защиты. Меры применяются для уменьшения числа внутренних антропогенных, техногенных и стихийных источников угроз. Основными организационными мерами являются:

выбор местоположения и размещения объекта информатизации;

физическая защита и организация охраны;

ограничение доступа в помещения, в которых установлены технические средства обработки информации;

подбор и работа с сотрудниками;

повышение профессиональный квалификации сотрудников;

организация инструктажа персонала;

организация учета оборудования и носителей;

контроль выполнения требований по защите;

противопожарная охрана;

обеспечение надежного сервисного обслуживания;

организация взаимодействия с другими подразделениями и организациями.

Устранение угроз организационными методами является наименее затратным мероприятием по защите информации.

К технологическим мерам защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

К данным мерам относятся:

- использование процедур двойного ввода ответственной информации;

- инициализации ответственных операций только при наличии согласования нескольких лиц;

- процедуры проверки реквизитов исходящих и входящих сообщений и т.п.

Инженерно-технические методы ориентированы на оптимальное построение зданий, сооружений, инженерных сетей и транспортных коммуникаций с учетом требований обеспечения информационной безопасности.

К инженерно-техническим мерам относятся:

- обеспечение электрозащиты оборудования и зданий;

- экранирование помещений;

- защита помещений от разрушений;

- оптимальное размещение оборудования;

- оптимальное размещение инженерных коммуникаций;

- применение средств визуальной защиты;

- акустическая обработка помещений;

- применение систем кондиционирования.

Технические меры основаны на применении специальных технических средств защиты информации, контроля обстановки и ориентированы на устранение угроз, связанных с действиями внешних угроз по воздействию на информацию техническими средствами.

Некоторые из этих мер позволяют устранить воздействие техногенных источников угроз и ослабляют влияние объективных, субъективных и случайных уязвимостей.

К техническим мерам относятся:

- резервирование технических средств обработки;

- резервирование каналов связи;

- использование выделенных каналов связи;

- создание резервной копии (дублирование) информационных ресурсов;

- создание системы пространственного зашумления;

- создание системы акустического и вибрационного зашумления;

- экранирование узлов и оборудования;

- использование источников гарантированного питания;

- контроль каналов связи для передачи информации;

- контроль отсутствия электронных устройств перехвата информации на объектах информатизации.

Программно-аппаратные меры предназначены для устранения проявления угроз, непосредственно связанных с процессом обработки информации.

Реализация программно-аппаратных мер существенно снижает влияние внутренних антропогенных источников угроз.

В группе программно-аппаратных мер объединяются такие меры, как:

- ограничение доступа к средствам обработки информации (ПО, техническим средствам);

- ограничение доступа к объектам защиты (защищаемой информации);

- разграничение доступа субъектов (пользователей);

- управление внешними и внутренними потоками информации;

- сокрытие структуры и назначения;

- подтверждение подлинности информации;

- преобразование (шифрование, кодирование) информации при её передаче и хранении;

- блокирование неиспользуемых сервисов;

- мониторинг целостности ПО, конфигурации ПО и аппаратных средств;

- антивирусная защита;

- мониторинг событий и инцидентов информационной безопасности;

- мониторинг действий пользователей корпоративной сети.

При предоставлении сторонним лицам доступа к информации и активам организации, следует обращать внимание на все установленные требования информационной безопасности и принять меры безопасности в отношениях с внешними пользователями.

Перед предоставлением доступа сторонним лицам к любым активам организации следует учесть следующие условия, относящиеся к информационной безопасности (в зависимости от типа и уровня предоставляемого доступа, из которых не все могут быть применены):

- защита активов, включающая:

1.1 процедуры по защите активов организации, в том числе информации и ПО, а также управление известными уязвимостями;

1.2 процедуры определения факта компрометации активов, например, вследствие потери или модификации данных;

1.3 целостность активов;

1.4 ограничения на копирование и раскрытие информации;

1.5 описание предоставляемых товаров и услуг;

1.6 различные предпосылки, требования и выгоды от доступа клиентов;

- соглашения по управлению доступом, охватывающие:

2.1 разрешенные методы доступа, а также управление и использование уникальных идентификаторов пользователей и паролей;

2.2 процесс предоставления привилегий и полномочий на доступ;

2.3 принцип запрета любого доступа, явно неразрешенного;

2.4 процесс отзыва прав доступа пользователей или блокирование доступа;

2.5 процедуры отчетности, уведомления и расследования инцидентов нарушения информационной безопасности и выявления слабых звеньев системы безопасности;

2.6 описание каждого сервиса, предназначенного для доступа;

2.7 плановый уровень сервиса и недопустимые уровни сервиса;

2.8 право мониторинга и отмены любой деятельности, связанной с активами организации;

2.9 соответствующие обязательства организации и клиента;

2.10 обязанности, касающиеся юридических вопросов и способов обеспечения соответствия требованиям законодательства, например, законов о защите данных, принимая во внимание различные национальные законодательные системы, в случае, если соглашение включает сотрудничество с клиентами за рубежом;

2.11 права на интеллектуальную собственность и авторские права, а также защита любой совместной работы.

Требования информационной безопасности, относящиеся к сотрудникам сторонних организаций, получающим доступ к активам организации, могут значительно различаться в зависимости от классификации предоставляемой информации и средств ее обработки. Данные требования безопасности могут быть отражены в контракте, заключаемом с сотрудником сторонней организации, который содержит все определенные риски и требования информационной безопасности.

Контракт со сторонними организациями также может содержать и другие требования безопасности. В контракте на предоставление доступа сторонней организации, необходимо указывать разрешение на привлечение других приемлемых сторон, а также условия их доступа и участия.

12. Раздел **«Реагирование на инциденты информационной безопасности»** должен содержать описание процесса реагирования на инциденты информационной безопасности, который должен включать средства системного аудита для автоматизированных участков обработки информации, а также регламент представления отчетов об инцидентах в области информационной безопасности для всего персонала организации и другую информацию о состоянии системы защиты.

В данном разделе должны быть описаны механизмы реагирования на инциденты, например, информация об обнаружении инцидентов нарушения информационной безопасности докладывается руководству и сообщается администратору информационной безопасности в установленном порядке. Запрещается принятие самостоятельных и несанкционированных действий, не регламентированных документами или соответствующими инструкциями.

При обнаружении каналов утечки информации, проводятся мероприятия по локализации участка обработки информации в целях пресечения дальнейшей утечки, а также приостанавливаются процессы, связанные с обработкой защищаемой информации в организации. В случае заражения вредоносными программами проводятся мероприятия по устранению нанесённого ущерба, согласно «Инструкции по антивирусной защите организации».

В целях эффективного управления инцидентами в организации, в данном разделе следует описать обязанности и порядок эффективной безотлагательной обработки событий и слабых мест информационной безопасности. В качестве реакции на них следует применять процессы непрерывного усовершенствования, отслеживания, оценки и полного управления инцидентами информационной безопасности.

Для обеспечения быстрого, эффективного и организованного реагирования на инциденты информационной безопасности, следует разработать и утвердить порядок управления инцидентами.

Для обнаружения инцидентов информационной безопасности, кроме сообщений о событиях и уязвимостях информационных систем, следует производить мониторинг систем, оповещений и уязвимостей.

Цели управления инцидентами информационной безопасности необходимо согласовывать с руководством, доводить до сведения персонала, отвечающих за управление инцидентами информационной безопасности, приоритетов организации по обращению с инцидентами.

Инциденты информационной безопасности могут выходить за рамки организации. Необходимо установить механизм координации всех действий, связанных

с реагированием на инциденты, даже если это касается вопроса обмена информацией о данных инцидентах с внешними организациями.

13. Раздел **«Обеспечение безопасности каналов связи»**. Защита проводных каналов связи должна быть направлена на снижение вероятности несанкционированного доступа к информации, путем гальванического подключения к информационным кабелям или снятия информации через побочные электромагнитные излучения и наводки на другие кабели, а также на обеспечение защиты кабельного оборудования от электромагнитных помех и механического повреждения.

Защита беспроводных каналов связи должна быть направлена на снижение таких атак, как прослушивание трафика, отказ в обслуживании, несанкционированное подключение.

14. Раздел **«Распределение ответственности»**. Данный раздел является одним из важных разделов политики и должен отражать принципы управления информационной безопасности организации со стороны руководства, распределение обязанностей, а также координацию вопросов информационной безопасности.

Все обязанности по обеспечению информационной безопасности должны быть четко определены в данном разделе.

Основными обязанностями руководства организации при обеспечении информационной безопасности являются:

- определение целей обеспечения информационной безопасности, соответствующих требованиям организации;

- формулировка, пересмотр и утверждение политики;

- контроль эффективности внедрения политики;

- обеспечения четкого руководства и ощутимой административной поддержки инициативам, направленным на повышение безопасности;

- выделения необходимых средств информационной безопасности;

- назначение ответственных за информационную безопасность в пределах организации и их обязанности;

- инициирование планов и программ поддержания осведомленности персонала по информационной безопасности.

Кроме того, необходимо осуществлять следующие мероприятия:

- установить и четко определить обязанности ответственного персонала, связанные с каждыми отдельными информационными системами и ресурсами, а также лиц, контролирующих их действия;

- назначить ответственного за каждый актив и процесс безопасности, а также задокументировать данные обязанности;

- разграничить полномочия ответственного персонала и утвердить в установленном порядке;

- определить критические активы и процессы безопасности, а также документировать их.

Необходимо назначить ответственного из числа руководства организации, который будет отвечать за все вопросы, связанные с обеспечением информационной безопасности в организации.

Руководителям различных заинтересованных подразделений организации следует координировать вопросы внедрения мероприятий по управлению информационной безопасностью.

Координация вопросов информационной безопасности должна включать взаимодействие и сотрудничество руководства, пользователей, администраторов,

разработчиков приложений, аудиторов и персонала безопасности, а также специалистов с навыками в таких областях, как страхование, юриспруденция, кадровая работа, управление информационными технологиями или рисками. С учетом этого в данном разделе политики следует отразить меры по:

- оценке мер информационной безопасности на соответствие с утвержденной политикой;

- определению способов обработки случаев несовместимости;

- утверждению методологии и процессов обеспечения информационной безопасности, например, определение рисков, классификации информации;

- определению значимых изменений угроз и моменты, когда информация и средства ее обработки подвергаются угрозам;

- оценке адекватности и координации внедрения средств управления информационной безопасностью;

- эффективности проводимого в масштабах организации обучения, тренингов и осведомленности по вопросам информационной безопасности;

- анализу информации, полученной в результате выявления и обработки инцидентов информационной безопасности, а также рекомендовать приемлемые меры в ответ на установленные инциденты информационной безопасности.

В данном разделе также необходимо определить механизмы подписания и пересмотра соглашений о соблюдении конфиденциальности, разработанного на основании действующей в организации политики.

Соглашения о соблюдении конфиденциальности должны отвечать требованиям по защите конфиденциальной информации, закрепленным в нормативно-правовых актах. При определении требований к соглашениям о соблюдении конфиденциальности следует руководствоваться следующими аспектами:

- классификация защищаемой информации (например, конфиденциальная информация);

- ожидаемый срок действия соглашения, включая случаи, когда соблюдение конфиденциальности может быть бессрочным;

- необходимые меры, в случае прекращения действия соглашения;

- ответственность и действия лиц, подписывающих соглашение, во избежание несанкционированного разглашения информации (такие как «принцип необходимого знания», «знать только то, что необходимо»);

- обязанности и права лиц, подписывающих соглашение, при допуске к использованию конфиденциальной информации;

- проведение аудита и мониторинга использования конфиденциальной информации;

- порядок донесения и отчетности о случаях несанкционированных разглашений и нарушений конфиденциальности;

- определение сроков, когда информация должна быть уничтожена или возвращена, в случае прекращения действия соглашения;

- применяемые меры, в случае нарушения соглашения.

На основании требований политики, в организации может возникнуть необходимость в других соглашениях о соблюдении конфиденциальности и неразглашении.

Соглашения о соблюдении конфиденциальности и неразглашении должны соответствовать действующим требованиям.

Требования к соглашениям о соблюдении конфиденциальности информации следует при необходимости (при изменение действующего законодательство) пересматривать.

Соглашения о соблюдении конфиденциальности предназначены для защиты информационных активов организации. Лица, подписывающие данные соглашения, несут ответственность за несанкционированное использование и разглашение конфиденциальной информации.

При различных обстоятельствах организации могут понадобиться разные формы соглашений о соблюдении конфиденциальности, но все они должны отражать основные требования информационной безопасности.

15. Раздел **«Порядок пересмотра и актуализации политики»** определяет процедуру по пересмотру и актуализации политики, а также порядок внесения изменений в политику. Также в данном разделе приводится информация (вид документа, регистрационный номер и другие атрибуты документа) о согласовании.

3.3. Содержание документов, входящих в состав политики информационной безопасности организации, или на которые приведены ссылки

Положение о корпоративной (локальной) сети и по организации защищенных сетевых соединений должно включать себя следующие разделы:

- общие положения;
- назначение корпоративной (локальной) сети;
- состав корпоративной (локальной) сети;
- принцип действия корпоративной (локальной) сети;
- организация работ по сопровождению, развитию корпоративной (локальной) сети организации;
- развитие корпоративной (локальной) сети организации;
- классификация защищенных соединений (VPN, SSL, SSH и т.д.);
- использование защищенных соединений;
- принципы организации защищенных соединений.

Положение об обеспечении информационной безопасности на уровне сетевой инфраструктуры и межсетевое экранирование должно включать в себя следующие разделы:

- общие требования по обеспечению информационной безопасности с применением межсетевых экранов;
- процедуры внесения изменений в программное обеспечение и конфигурацию межсетевых экранов;
- порядок проведения испытаний на контрольных стендах и опытная эксплуатация;
- порядок ввода изменений в эксплуатацию.

При этом должны быть учтены требования O‘zDSt 2815.

Инструкция системного администратора локальной (корпоративной) сети должна включать в себя следующие разделы:

- общие положения;
- права системного администратора корпоративной сети;
- обязанности и ответственность системного администратора корпоративной сети.

Положение об отделе обеспечения информационной безопасности (инструкция администратора информационной безопасности) локальной (корпоративной) сети должно включать в себя следующие разделы:

- общие положения;

- основные задачи и функции отдела;

- права и обязанности, ответственность;

- администратор информационной безопасности, права, обязанности и ответственность.

Положение по обновлению системного и прикладного программного обеспечения, а также резервному копированию и восстановлению данных должно включать в себя следующие разделы:

- общие положения;

- задачи по установке, внесению изменений, конфигурированию и обновлению ПО;

- ответственность за обновление системного и прикладного ПО;

- классификацию типов резервного копирования;

- порядок резервного копирования и восстановления информации;

- контроль результатов резервного копирования;

- перечень резервируемой информации;

- резервное копирование.

Инструкция по парольной защите должна включать в себя следующие разделы:

- общие положения;

- организационно-техническое обеспечение процессов генерации паролей;

- процесс смены и прекращения действия паролей в информационной системе организации;

- контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

Инструкция по антивирусной защите должна включать в себя следующие разделы:

- основные положения;

- организация работ по антивирусной защите;

- требования к участникам работ по антивирусной защите;

- ответственность участников работ по антивирусной защите.

Инструкция по обеспечению безопасности при работе со съемными носителями данных, мобильными устройствами, накопителями данных должна включать в себя следующие разделы:

- общие положения;

- правила применения съемных носителей в организации;

- ответственность за утерю и несанкционированное использование.

Правила по разработке матрицы доступа к информационным ресурсам автоматизированной системы должны описывать процедуру разработки матрицы доступа к информационным ресурсам организации.

Доступом к информации и средствам обработки информации следует управлять на основе требований к безопасности.

Следует определять, документально оформлять и пересматривать политику управления доступом, на основании требований деятельности организации к безопасности.

В данном документе следует четко сформулировать правила управления доступом и права для каждого пользователя или группы пользователей. Средства

управления доступом бывают логическими и физическими, их нужно рассматривать комплексно. Необходимо, чтобы в документе было учтено следующее:

- требования к безопасности конкретных информационных систем и ресурсов;
- идентификация всей информации, связанной с функционированием конкретных информационных систем, ресурсов и рисков, с которыми сталкиваются пользователи;
- условия распространения информации, авторизации доступа, а также классификация информации и требуемые уровни ее защиты;
- согласованность между политиками управления доступом и классификацией информации, применительно к различным системам и сетям;
- существующее законодательство и любые договорные обязательства, относительно защиты доступа к данным или сервисам;
- стандартные профили доступа пользователей для типовых обязанностей и ответственности в организации;
- управление правами доступа в распределенной сети, с учетом всех типов доступных соединений;
- разделение ролей управления доступом, например, запрос на доступ, разрешение доступа, администрирование доступа;
- требования формального санкционирования запросов на доступ;
- требования периодического пересмотра средств управления доступом;
- изъятие прав доступа.

При определении правил управления доступом следует принимать во внимание следующее:

- различия между обязательными и рекомендуемыми для использования правилами, которые применяются при определенных условиях;
- формулировать правила, основываясь на предпосылке «все должно быть в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»;
- изменения уровня конфиденциальности информации, генерируемых автоматически средствами обработки информации и инициируемых по усмотрению пользователей;
- изменения прав пользователя, устанавливаемых автоматически информационной системой и определенных администратором;
- правила, требующие и не требующие специального согласования перед введением в действие.

Правила управления доступом следует поддерживать с помощью формального порядка и четко определенных обязанностей.

Должна быть описана процедура разработки матрицы доступа к информационным ресурсам организации. Администратором в соответствии с уровнем допуска персонала к информации разрабатывается матрица доступа к информационным ресурсам, которая утверждается руководством организации.

Разработка матрицы доступа к информационным ресурсам автоматизированной системы осуществляется по следующему методу:

- формируется список информационных ресурсов (файлы, папки, устройства, службы, базы данных);
- формируются списки пользователей, с указанием уровня доступа – полномочий к информации.

Необходимо, чтобы порядок охватывал все стадии жизненного цикла доступа пользователей, начиная с регистрации в системе новых пользователей и заканчивая удалением учетных записей пользователей, которым больше не требуется доступ к информационным системам и сервисам. Особое внимание следует уделять мероприятиям в отношении предоставления прав привилегированного доступа,

с помощью которых пользователи могут обходить средства контроля системы. Типовые правила по разработке матрицы доступа к информационным ресурсам автоматизированной системы организации приведены в приложении № 1 к настоящему Методическому пособию.

Необходимо определить порядок получения разрешения на использование новых средств обработки информации.

Для внедрения процедур получения разрешения должны выполняться следующие мероприятия:

- новые средства и их назначение должны быть утверждены руководством организации и согласованы с администратором, ответственным за сопровождение безопасной среды функционирования локальных информационных систем. Эти меры позволяют гарантировать выполнение соответствующих политик и требований безопасности;

- необходимо проводить тестирование программно-аппаратных средств на совместимость с другими компонентами системы до момента внедрения;

- использование личных технических средств информатизации (например, ноутбуков, домашних компьютеров и т.д.) на рабочем месте для обработки служебной информации должно быть запрещено.

Перечень разрешенного к использованию программного обеспечения должен содержать таблицу со списком ПО, которое должно быть установлено на компьютере пользователей.

Инструкция по работе с сетью Интернет и корпоративной электронной почтой должна включать в себя следующие разделы:

- основные положения;
- основные требования к пользователям сети Интернет;
- разграничение прав и обязанностей;
- получение и распространение информации с помощью сети Интернет;
- правила использования корпоративной почты;
- ответственность персонала.

Порядок управления информационными активами организации должен включать в себя следующие разделы:

- основные положения;
- ответственность за информационные активы;
- владение информационными активами;
- допустимое использование информационных активов;
- ответственность за информационные активы;
- классификация информации;
- основные принципы классификации информации;
- порядок инвентаризации защищаемой информации;
- маркировка и обработка информации.

Все основные информационные активы организации должны быть учтены и закреплены за ответственными владельцами.

В данном документе необходимо идентифицировать владельцев всех основных активов и определить их ответственность за поддержание соответствующих мероприятий по управлению информационной безопасностью. Осуществление мероприятий по управлению информационной безопасностью может быть делегировано, но ответственность должна оставаться за назначенным владельцем актива.

Данным документом вся информация и активы, связанные со средствами обработки информации, должны быть закреплены назначенному подразделению организации.

Должны быть установлены меры ответственности владельцев активов, такие как:

- обеспечение соответствующей классификации информации и активов, связанных со средствами обработки информации;
- разграничение и периодический пересмотр ограничений и классификации доступа, на основании действующей политики управления доступом.

Владеть можно:
- процессами обработки информации;
- определенным набором действий;
- приложениями;
- определенным набором данных.

Повседневные задачи могут быть делегированы, например, оператору, ежедневно следящему за активами, но ответственность остается за владельцем.

В сложных информационных системах, возможно, полезно будет определить группы совместно действующих активов, предоставляющих такие специфичные функции, как «сервисы». В таком случае владелец сервиса является ответственным за предоставление сервиса, включая работу активов, его предоставляющих.

Данным документом следует четко установить, задокументировать и внедрить правила допустимого использования информации и активов, связанных со средствами обработки информации.

Классификация информации необходима для определения требований к защите информации, является необходимым элементом организации работ по обеспечению информационной безопасности и имеет своими целями:

- создание нормативно-методической основы для дифференцированного подхода к защите ресурсов автоматизированной системы (информации, задач, рабочих мест, серверов, компьютеров) на основе их классификации по степени риска в случае нарушения их доступности, целостности или категорий доступа;
- типизацию принимаемых организационных мер и распределения аппаратно-программных средств защиты ресурсов по компьютерам и серверам организации и унификацию вариантов настроек средств защиты.

Исходя из необходимости обеспечения различных уровней защиты разных видов информации, хранимой и обрабатываемой в организации, а также с учетом возможных путей нанесения ущерба организации, другим организации или персоналу, вводятся категории доступа, целостности и доступности защищаемых информационных ресурсов.

Информационные ресурсы по категориям доступа разделяются на общедоступные информационные ресурсы и информационные ресурсы с ограниченным доступом:

- общедоступными информационными ресурсами являются информационные ресурсы, предназначенные для неограниченного круга пользователей;
- к информационным ресурсам ограниченного доступа относятся информационные ресурсы, содержащие информацию о государственных секретах и конфиденциальную информацию или информацию, доступ к которой ограничен организацией.

Категории целостности защищаемой информации:

- «ВЫСОКАЯ» (В) - к данной категории относится информационный ресурс, несанкционированная модификация или фальсификация которого может привести к нанесению значительного прямого ущерба организации, целостность которого

должна обеспечиваться гарантированными методами (например, средствами электронной цифровой подписи) в соответствии с обязательными требованиями законодательства, приказов, директив и других нормативных актов;

- «НИЗКАЯ» (Н) - к данной категории относится информационный ресурс, несанкционированная модификация или фальсификация которого может привести к нанесению незначительного косвенного ущерба организации, целостность которого должна обеспечиваться в соответствии с решением руководства организации (методами подсчета контрольных сумм, хеш-функций и т.п.);

- «НЕТ ТРЕБОВАНИЙ» (-) - к данной категории относится информационный ресурс, к обеспечению целостности которого требований не предъявляется.

Категории доступности защищаемых информационных ресурсов:

- «БЕСПРЕПЯТСТВЕННАЯ ДОСТУПНОСТЬ» (Б) – доступ к информационному ресурсу должен обеспечиваться в любое время (задержка не должна превышать нескольких секунд или минут);

- «ВЫСОКАЯ ДОСТУПНОСТЬ» (В) – доступ к информационному ресурсу должен осуществляться без существенных временных задержек (задержка не должна превышать нескольких часов);

- «СРЕДНЯЯ ДОСТУПНОСТЬ» (С) – доступ к информационному ресурсу может обеспечиваться с существенными временными задержками (задержка не должна превышать нескольких дней);

- «НИЗКАЯ ДОСТУПНОСТЬ» (Н) – временные задержки при доступе к информационному ресурсу практически не лимитированы (допустимая задержка получения результата - несколько недель).

Категорирование информации проводится на основе их регистрации (инвентаризации) и предполагает составление и поддержание в актуальном состоянии перечней информации (информационных ресурсов) организации, подлежащих защите.

Отнесение информации к государственным секретам осуществляется согласно законодательству.

К конфиденциальной информации относятся несекретные сведения ограниченного распространения, предусмотренные Перечнем сведений, отнесенных к конфиденциальной информации, согласно приложению №2 постановления Кабинета Министров Республики Узбекистан от 7 ноября 2011года №296 «О мерах по реализации Постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572».

Ответственность за определение уровня конфиденциальности (грифа) информации (информационного ресурса) возлагается на исполнителя документа, за составление и ведение учета документальной информации, контроль за правильностью определения грифа и за составление, ведение перечней информационных ресурсов организации возлагается на канцелярию организации.

Ответственность за составление и ведение перечней информационных ресурсов организации возлагается:

- в части составления и ведения перечня автоматизированных систем (с указанием их размещения, закрепления за структурными подразделениями организации, состава и характеристик входящих в его состав технических средств) - на ответственных за информационную безопасность в организации;

- в части составления и ведения перечня информационных ресурсов автоматизированных систем (с указанием перечней категорий доступа, целостности, доступности и используемых при их решении ресурсов - каталогов, файлов с информацией) - на пользователя автоматизированной системы.

Ответственность за установление требуемого уровня защищенности, в зависимости от категории информационных ресурсов автоматизированной системы организации, возлагается на администратора информационной безопасности.

Следует определить и внедрить соответствующий набор процедур для маркировки информации при её обработке, в соответствии с системой классификации, принятой организацией.

Процедуры маркировки должны относиться к информационным активам, представленным как в физической, так и в электронной форме.

При осуществлении вывода данных из систем следует использовать соответствующий гриф секретности или другой гриф согласно законодательству. В маркировке следует отражать уровень классификации. Следует маркировать напечатанные отчеты, экранные формы, носители информации (ленты, диски, компакт-диски, кассеты), электронные сообщения и передаваемые файлы.

Для каждого уровня классификации следует определить порядок обращения, включая безопасную обработку, хранение, передачу, деклассификацию и уничтожение. Также следует включить процедуры «цепочки поставок» и фиксировать в журнале любые события, относящиеся к безопасности.

В соглашения с другими организациями, предусматривающие совместное использование информации, следует включать порядок установления классификации данной информации и интерпретации меток классификации другой организации.

Маркировка и безопасное обращение с классифицированной информацией являются основным требованием к соглашениям по совместному использованию информации. Обычной формой маркировки являются физические метки. Однако некоторые информационные активы, такие, как документы в электронном виде, не могут быть маркированы физически, поэтому необходимо использовать электронные средства, например, уведомляющие метки, которые могут появляться на экранах или дисплеях. В случае нецелесообразности использования маркировки, могут быть применены другие средства назначения уровня классификации информации.

В целях обеспечения надлежащий защиты информационных ресурсов, в организации должен вестись учет всех информационных ресурсов. Для этого все ресурсы должны быть идентифицированы и сформированы, а также должен поддерживаться в актуальном состоянии Реестр информационных ресурсов автоматизированных систем организации (далее – Реестр), пример заполнения которого, приведен в приложении №2к настоящему Методическому пособию.

Реестр должен включать в себя всю информацию, необходимую для восстановления после катастрофы, включая тип ресурса, его формат, размещение, информацию о резервных копиях и категориях. Этот Реестр не должен без необходимости дублировать другие реестры, но при этом должна быть обеспечена согласованность их содержимого. Для этого, после регистрации ресурса в канцелярии, присвоенный номер списывается на Реестр автоматизированной системы, в котором размещается ресурс.

Реестр представляет собой документ (на бумажном или электронном носителе), который регистрируется в канцелярии организации и содержит все информационные ресурсы организации, подлежащие защите. По решению руководителя организации, Реестр может вестись для всей организации, либо для его структурной единицы.

Для всех информационных ресурсов должны быть назначены их владельцы, на которых возлагается ответственность за обеспечение безопасности этих ресурсов.

Владелец ресурса несет ответственность за обеспечение правильной категоризации ресурса, определение и периодического пересмотра категорий и прав доступа к этому ресурсу.

В случае необходимости, владельцы ресурсов могут делегировать ответственность за реализацию и сопровождение механизмов контроля другому персоналу организации, однако ответственность за обеспечение надлежащей защиты ресурса при этом остается за его владельцем.

При инвентаризации информационных ресурсов их сохранность проверяется согласно Реестру и фактическому наличию по указанному в Реестре их местоположения.

Инструкция по организации технической защиты информации должна включать в себя информацию об используемых методах и средствах технической защиты информации в организации.

Инструкция по организации криптографической защиты информации должна включать в себя информацию об используемых методах и средствах криптографической защиты информации в организации.

Порядок обращения с информацией, подлежащей защите должен содержать перечень информационных ресурсов, неправильное обращение с которыми может нанести ущерб организации, требования по обращению с данными информационными ресурсами, ответственность за нарушение и соглашение (обязательство) о соблюдении данных требований.

План обеспечения непрерывной работы и восстановления работоспособности организации в чрезвычайных (нештатных) ситуациях должен включать в себя следующие разделы:

- Общие положения и основные понятия;
- Общие требования;
- Средства обеспечения непрерывной работы и восстановления;
- Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению информационных систем.

Приложение № 1

Типовые правила по разработке матрицы доступа к информационным ресурсам автоматизированной системы организации

I. Общие положения

1.1. Типовые правила описывают процедуру разработки матрицы доступа к информационным ресурсам организации.

1.2. Администратором, в соответствии с уровнем допуска персонала к информации, разрабатывается матрица доступа к информационным ресурсам многопользовательской автоматизированной системы, которая утверждается руководством организации.

II. Разработка матрицы доступа

Разработка матрицы доступа к информационным ресурсам информационной системы осуществляется по следующему методу:

1) формируется список информационных ресурсов (файлы, папки, устройства, службы, базы данных);

2) формируются списки пользователей, с указанием уровня доступа – полномочий к информации:

- Read (R) - получение информации из объекта;
- Write (W) - обновление информации в объекте;
- Append (A) - добавление в объект новой информации (не изменяя старой);
- Execute (E) - интерпретация объекта как исполняемого кода;
- Delete (D) - уничтожение объекта;
- Getinfo (G) - получение информации об объекте;
- Setinfo (S) - установка информации об объекте;
- Privilege (P) - установка прав доступа к объекту.

Пример приведен в таблице 1.

Таблица 1

Наименование файла	Администратор	Пользователь №1	Пользователь № 2	Пользователь № 3
	(Полномочия)	(Полномочия)	(Полномочия)	(Полномочия)
Наименование каталога	Администратор	Пользователь № 1	Пользователь № 2	Пользователь № 3
	(Полномочия)	(Полномочия)	(Полномочия)	(Полномочия)
Наименование устройства	Администратор	Пользователь № 1	Пользователь № 2	Пользователь № 3
	(Полномочия)	(Полномочия)	(Полномочия)	(Полномочия)
Наименование базы данных	Администратор	Пользователь № 1	Пользователь № 2	Пользователь № 3
	(Полномочия)	(Полномочия)	(Полномочия)	(Полномочия)

Приложение №2

Реестр информационных ресурсов организации (структурной единицы организации)

Таблица1

№	Регистрационный номер	Название ресурса	Описание ресурса	Размещение	Использование	Формат	Уровень конфиденциальности[1]	Целостность[2]	Доступность[3]	Частота обновления данных	Пользователи[4]	Владелец[5]
1		Данные персонала	Резюме, паспортные данные, штатное расписание, должностные инструкции и т.п.	Компьютер № каталог, файл	Управление персоналом	*.doc	ДСП	В	В	1 неделя		
2		Резервные копии данных персонала	Носитель №	Сейф №	Восстановление данных	CD, DVD	ДСП	–	–	1 неделя		
3		База данных учета	Вся бухгалтерская информация	офисная сеть	Бухгалтерский и налоговый учет	*.db	ДСП	В	В	1 день		
4		Финансовые данные по	Зарплатные ведомости	Компьютер № каталог, файл	Управление персоналом	*.xls	ДСП	В	С	1 месяц		

		персоналу										
5		Системные образы		Сейф № 1	Установка и восстановление систем	CD, DVD	–	–	–	-		Администратор
6		Файлы конфигурации	Лог-файлы сервера № 1	Сервер № 1	Восстановление конфигурации	Zip	–	–	–	1 неделя		Администратор
7		Дистрибутивы ПО		Сервер № 2	Установка и восстановление систем	CD, DVD	-	–	–	1 день		Администратор
8		Сайт организации	http://domen.uz	Сервер № 3		*.html	_	-	С	1 час		Администратор
9		Сайт отдела	http://d2.domen.uz	Сервер № 3		*.html	_	-	С	1 час		Администратор

[1]Уровень Конфиденциальности: СС (Совершенно секретно), С (Секретно), ДСП и н/с;
[2]Целостность: В, Н – (нет требований);
[3]Доступность: Б, В, С, Н;
[4]Пользователи: ФИО персонала, которому санкционирована работа с ресурсом на основе матрицы доступа;
[5]Владелец: ФИО персонала, ответственного за информационный ресурс (в соответствии с приложением А)

Приложение № 3

Перечень нормативно-правовых актов и нормативных документов, регламентирующих деятельность в области обеспечения информационной безопасности

[1] O‘zDSt 1047:2003 Информационные технологии. Термины и определения

[2] O‘zDSt 2927:2015 Информационная технология. Информационная безопасность.Термины и определения

[3] O‘zDSt 2814:2014 Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации

[4] O‘zDSt 2815:2014 Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации

[5] O‘zDSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь

[6] O‘zDSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

[7] O‘zDSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

[8] O‘zDSt ISO/IEC 27003:2014 Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью

[9] O‘zDSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности

[10] O‘zDSt ISO/IEC 27007:2015 Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью

[11] O‘zDSt ISO/IEC 27008:2015 Информационная технология. Методы обеспечения безопасности. Руководство для аудиторов по средствам управления информационной безопасностью

[12] O‘zDSt ISO/IEC 27010:2015 Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и между организациями

[13] O‘zDSt ISO/IEC 27035:2015 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности

[14] O‘zDSt ISO/IEC-1:2008 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

[15] O‘zDSt ISO/IEC-2:2008 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть2. Функциональные требования безопасности

[16] O‘zDSt ISO/IEC-3:2008 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности