

ПОЛОЖЕНИЕ О ЛОКАЛЬНОЙ СЕТИ ПО ОРГАНИЗАЦИИ ЗАЩИЩЕННЫХ СЕТЕВЫХ СОЕДИНЕНИЙ

1. Назначение

Локальная сеть УИТ является неотъемлемой частью системы управления и предназначена для решения задач управления на базе современных информационных технологий, обеспечивающих, в частности, ускорение принятия решений на основе:

- оперативного обмена данными между отделами УИТ;
- использование общих информационных ресурсов сети;
- доступа через единую локальную сеть к данным других интра и глобальных сетей (Интернет);
- применение электронной почты;
- организации централизованного хранилища данных с различным уровнем доступа к информации;
- отслеживание изменений данных в реальном масштабе данных.

2. Состав

Локальная сеть образуют базовые компоненты оборудования, программного обеспечения и параметров сетевого и межсетевого взаимодействия:

1. Сервера: файловые, баз данных, приложений, почтовые, архивные, удаленного доступа, печати;
2. Телекоммуникационная инфраструктура: кабели, соединительные устройства, устройства расширения (и ограничения) доступа;
3. Рабочие станции с необходимыми сетевыми адаптерами;
4. Системы дублирования и хранения информации;
5. Системы бесперебойного питания серверов и рабочих станций;
6. Информационная инфраструктура: операционные системы, протоколы сетевого и межсетевого взаимодействия, прикладное программное обеспечение коллективного доступа, прикладное программное обеспечение рабочих станций.

3. Организация работ по сопровождению, развитию локальной сети

Все вопросы, касающиеся функционирования и расширения локальной сети решаются системным администратором.

Для оптимизации функционирования локальной сети системный администратор имеет право анализировать работу любого элемента входящего в состав сети.

Для устойчивой работы сети в целом, необходимо учитывать рекомендации системного администратора по реконфигурированию элементов, входящих в состав сети.

Все изменения и неисправности в обязательном порядке регистрируются в «Журнале работы локальной сети» ответственным сотрудником по информационной безопасности.

Сервера

- Администрирование серверов производится системным администратором.
- Уровни доступа потребителей конфиденциальной информации регламентируются распоряжением ректора УИТ и реализуются совместно системным администратором и ответственным сотрудником по информационной безопасности.
- Отключение серверов или рабочих станций для технологических целей производится только системным администратором с обязательным предварительным уведомлением всех пользователей ресурсов данного сервера или рабочей станции.
- При отключении серверов или устранении на них возникших неисправностей, системный администратор обязан, в первую очередь, осуществить организационно-технические мероприятия (установка обходного пути, реплицирование БД и т.д.) по обеспечению неразрывности рабочего процесса подразделений.

Телекоммуникации

- Создание и сопровождение телекоммуникационных каналов сети является исключительной компетенцией УИТ.
- Подключение рабочих станций к сети производится системным администратором, либо уполномоченными техническими специалистами УИТ по заявкам соответствующих подразделений.
- Решение о подключении или реорганизации сегмента принимается системным администратором на основании заявки в соответствии с имеющимися ресурсами и техническими возможностями.
- Изменение топологии сети сторонними организациями или самостоятельно пользователем, подключение и реконфигурация любого элемента сети без согласования с системным

администратором и ответственным сотрудником по информационной безопасности запрещено.

- Подключение модемов и иных устройств на рабочих станциях для доступа в сеть извне запрещено. В исключительных случаях такие подключения осуществляет системный администратор, согласовывая свои действия с ответственным сотрудником по информационной безопасности с обязательным контролем этих рабочих станций.

Рабочие станции

- Настройка операционной системы рабочих станций пользователей для корректной работы сети производится системным администратором. Изменение конфигурации системы рабочих станций, установка новых программных продуктов и аппаратных средств, изменяющих настройки системы самостоятельно или сторонними лицами без участия системного администратора, сотрудника ИВЦ и ответственного сотрудника по информационной безопасности **запрещено**.
- Права и обязанности пользователей локальной сети регламентируются настоящим положением и должностными инструкциями.
- Ручное отключение пользователя сети от сетевых ресурсов производится с обязательным уведомлением данного пользователя.
- При любых изменениях конфигурации подключения пользователя, системным администратором производится обязательная проверка функционирования канала и доступа к ресурсам сети.
- Пользователям сети категорически **запрещено** передавать сторонним лицам какие-либо сведения о настройке элементов сети (имена пользователей, пароли и т.д.).
- Несанкционированное расширение пользователями своих или чужих прав **запрещено**.
- **Запрещено** изменять месторасположение рабочих станций без согласования.

В случае нарушения установленного порядка функционирования локальной сети виновные на основании рапорта системного администратора будут привлекаться к административной и материальной ответственности.

ОБЩИЕ РЕКОМЕНДАЦИИ И ПРАВИЛА ПОЛЬЗОВАНИЯ ЛОКАЛЬНОЙ СЕТЬЮ

Использование учетной записи:

Для надежной и безопасной работы в локальной сети администрация настоятельно рекомендует пользователям придерживаться следующих правил при работе с учетными записями:

1. Контролировать доступ к своей учетной записи, следить за содержимым своей общедоступной папки (если таковая имеется), за появлением файлов неизвестного происхождения (особенно скрытых).

ПОЛЬЗОВАТЕЛЯМ ЛОКАЛЬНОЙ СЕТИ КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ

1. Использовать вычислительную технику для несанкционированного доступа к другим компьютерам сети и нарушения системы безопасности в целом;
2. Подключать компьютеры к сети без специального разрешения системного администратора;
3. Категорически запрещается самовольно изменять IP-адреса компьютеров в сети, принадлежность компьютера к домену, сетевое имя компьютера, настройки шлюзов и основных серверов;
4. Распространять и использовать программное обеспечение и любые материалы, полностью или частично защищенные авторскими правами, без разрешения владельца;
5. Преднамеренно/непреднамеренно распространять компьютерные вирусы и зараженные ими файлы;
6. Перехватывать чужую информацию, передаваемую по сети;
7. Использовать программное обеспечение, ориентированное на нарушение системы безопасности сети ("тройанские кони", бэкдоры и другое шпионское программное обеспечение);
8. Обмениваться информацией, запрещенной действующим законодательством Республики Узбекистан: пропаганда насилия, разжигание расовых, национальных и религиозных распри, порнография, любая информация, несущая оскорбления и клевету, а также распространяемая с целью хищения чужих денежных

средств или имущества путем обмана или злоупотребления доверием;

9. Несанкционированный доступ (или его попытки) к закрытым ресурсам в сети. Участвовать в проведении "сетевых атак" и "сетевого взлома".

Эти действия определяются как:

- a. использование против компьютеров или оборудования компьютерных сетей специальных средств, позволяющих получить нелегальный доступ к содержащейся информации;
 - b. передача компьютерам или оборудованию компьютерных сетей бессмысленной или бесполезной информации, создающей паразитическую нагрузку на аппаратуру;
 - c. уничтожение/модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами или администраторами этого программного обеспечения или данных;
 - d. фальсификация своего сетевого адреса при передаче данных в сеть;
 - e. фальсификация контактной информации, предъявленной владельцам или администраторам ресурсов или сетей;
 - f. использование псевдонимов и анонимность, кроме случаев, когда право пользования соответствующими ресурсами или сетей разрешают анонимность при их использовании.
10. Сканировать порты на удаленных хостах. Это может быть расценено как попытка взлома, со всеми вытекающими последствиями;

Сканированием считается выдача запросов, в том числе и единичных, на предмет наличия того или иного сервиса или опрос наличия работающих машин на группу адресов, либо опрос диапазона портов с целью определения работающих сервисов на одной машине или группе машин, а также выдача запросов, обработка которых не санкционирована принимающей стороной, не предусматривается сетевым сервисом или не разрешена администрацией ресурса.

11. Сканировать диапазоны IP-адресов (всю легально предоставляемую информацию об удаленной сети можно получить средствами DNS, traceroute и т.п.);

- 12.Использовать сеть во вред другим пользователям, путем самостоятельного или с помощью третьих лиц, вмешательства в действие аппаратуры и оборудования, а также иным способом;
- 13.Использовать доступ к компьютерным сетям для создания "сетевого шума" или "спама";
- 14.Рассылать не затребованную информацию по e-mail (спам), писем с указанием чужого адреса отправителя, писем угрожающего или оскорбляющего характера, "mailbombing", т.е. отправку писем, переполняющих почтовый ящик получателя и препятствующих получению новой почты;
- 15.Распространять информацию, оскорбляющую честь и достоинство других пользователей и персонала компьютерных сетей;
- 16.Физически повреждать оборудование сети;
- 17.Устанавливать серверные операционные системы без специального разрешения системного администратора;
- 18.Пользователям, работающим с конфиденциальными документами категорически запрещается пользоваться на рабочем месте различного рода мессенджерами (ICQ, MSN, Miranda, QIP, Mail.Ru агентами, Google messenger и т.д.);
- 19.Просмотр видео и прослушивание аудио через сеть, за исключением случаев, связанных со служебной необходимостью;
- 20.Хранение на локальных и публичных сетевых дисках файлов, не относящихся к выполнению служебных обязанностей сотрудника (игры, видео, музыку, фотографии, виртуальные CD и т.п.);
- 21.Просмотр в рабочее время сайтов развлекательной направленности и сайтов, содержание которых не относится напрямую к служебным обязанностям работника;
- 22.Играть в рабочее время в онлайн игры;
- 23.Устанавливать нелицензионное программное обеспечение, а также свободно распространяемое (FreeWare) программное обеспечение, способное нарушить работу локальной сети;
- 24.Разрабатывать или распространять любые виды компьютерных вирусов, «троянских коней» или «логических бомб»;
- 25.Открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на

переносных носителях без предварительной проверки
антивирусной программой.

- 26. Самовольная организация доступа к локальной сети УИТ через
машины конечных пользователей или другие устройства.
- 27. Использование различных сайтов анонимайзеров;
- 28. Использовать локальную сеть в деятельности, противоречащих
законодательству Республики Узбекистан.

ИНСТРУКЦИЯ СИСТЕМНОГО АДМИНИСТРАТОРА ЛОКАЛЬНОЙ СЕТИ

1. Общие положения

Системный администратор локальной сети УИТ – лицо, в исключительную компетенцию которого входят все вопросы, касающиеся программно-аппаратной стороны функционирования локальной сети и организационно-технические мероприятия по защите целостности и конфиденциальности всей информации, хранящейся либо передаваемой в электронном виде по локальной сети УИТ (совместно с администратором по информационной безопасности).

Системный администратор является сотрудником Информационно-вычислительного центра (ИВЦ) УИТ и подчиняется начальнику ИВЦ.

2. Права

Системный администратор имеет право:

- анализировать работу любых элементов сети для оптимизации её функционирования;
- отключать любые элементы при реконфигурировании, регламентном техническом обслуживании или устранении неисправностей;
- изменять параметры настройки элементов локальной сети при производственной необходимости, либо при внедрении новых технологий;
- расширять существующую сеть в соответствии с утвержденным планом её развития.

3. Обязанности

Системный администратор обязан:

- поддерживать максимальную работоспособность и внедрение новых элементов сети и проводить регламентные организационно-технические мероприятия по обслуживанию элементов сети и плановые работы по её расширению;
- совместно с администратором по информационной безопасности обеспечить максимально возможную защиту от несанкционированного доступа всей информации, передающейся по сети и хранящейся на серверах и рабочих станциях;

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УИТ

- обеспечить максимальную целостность и защиту от поражения компьютерными вирусами любой информации, передающейся по сети и хранящейся на серверах и рабочих станциях;
- принимать участие в создании нового прикладного программного обеспечения, если оно, либо его части предназначены для использования на элементах сети;
- документировать все изменения конфигурации элементов сети в «Журнал работы локальной сети» и информировать об этом администратора по информационной безопасности;
- рассматривать целесообразность применения новых технологий для увеличения эффективности функционирования сети;
- проводить инструктаж пользователей по внедряемым в использование технологиям или прикладному программному обеспечению, если это требует от пользователей дополнительных навыков и знаний. (Разрешается инструктаж не только в устной форме, но и в письменном, либо электронном виде путем создания инструкций, файлов справок, описаний, руководств пользователя и прочее, с последующим обязательным доведением до каждого пользователя.)

ПОЛОЖЕНИЕ ПО ОБНОВЛЕНИЮ СИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ РЕЗЕРВНОМУ КОПИРОВАНИЮ И ВОССТАНОВЛЕНИЮ ДАННЫХ

1. Общие положения

1.1 Настоящее Положение по обновлению системного и прикладного программного обеспечения, а также резервного копированию и восстановлению данных, хранящихся в УИТ, разработано с целью:

- определения порядка резервного копирования данных для последующего восстановления работоспособности ИС или её частей при полной или частичной потере информации, вызванной сбоями или отказами оборудования, нарушениями информационной безопасности, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

- определение должностных обязанностей лиц, занимающихся резервным копированием данных.

1.2 В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий.

1.3 Резервному копированию подлежат данные следующих основных категорий:

- данные, необходимые для восстановления работоспособности технологического оборудования (ОС, конфигурация системы);
- рабочие данные (базы данных, файлы).

1.4 Носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.5 Администратор по ИБ является ответственным за резервное копирования.

2. Классификация типов резервного копирования

2.1 По типу резервируемой информации:

- резервные копии рабочих данных;
- полные резервные копии файловой системы сервера.

2.2 По полноте сохраняемой информации:

- **Полное резервирование (Full backup)** — создание резервной копии всех подлежащих резервированию данных, необходимых для полного восстановления технологического оборудования;

- **Добавочное резервирование** (Incremental backup) — создание резервной копии всех данных, которые были модифицированы после предыдущего полного или добавочного резервирования;

- **Разностное резервирование** (Differential backup) — создание резервной копии всех данных, которые были изменены после предыдущего полного резервирования.

2.3 По способу доступа к носителю:

- **Оперативное резервирование** (Online backup) — создание резервного архива на постоянно подключенном (напрямую или через сеть) носителе.

- **Автономное резервирование** (Offline backup) — хранение резервной копии на съёмном носителе, кассете или картридже, который перед использованием следует установить в привод.

2.4 По времени выполнения резервной копии:

- резервные копии реального времени — данные резервируются непосредственно при их появлении в системе — при помощи репликации, распределенных хранилищ и т.п.

- плановые резервные копии — данные резервируются в заранее определенные моменты времени.

3. Порядок резервного копирования

3.1 Резервное копирование информации производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования;

- хранение архивов в соответствии с Методикой резервного копирования и восстановления данных (Таблица №2);

3.2 Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне резервируемых данных (Таблица №1), с заданной периодичностью. Методика резервного копирования и восстановления данных описана в Таблице №2.

3.3 Для исключения человеческого фактора и минимизации ущерба, связанного с восстановлением некорректных данных, система резервного копирования и восстановления должна быть автоматизирована с учетом минимального вмешательства контролирующего персонала.

3.4 О выявленных попытках несанкционированного доступа к процессу резервного копирования, сообщается руководству УИТ запиской в течение 1 рабочего дня после обнаружения указанного события.

3.5 Ответственный за резервное копирование должен обеспечивать:

- первоначальную настройку системы резервного копирования (создание расписаний, оповещений). Запуск в эксплуатацию системы резервного копирования;

- внесение существенных изменений в настройку системы резервного копирования;
- анализ журнала резервного копирования, отслеживание необходимости изменений настроек резервного копирования;
- контроль резервного копирования или оборудования;
- восстановление данных с резервных копий.

4. Контроль результатов резервного копирования

4.1 Контроль результатов всех процедур резервного копирования осуществляется администратором с частотой, определяемой критичностью данных, согласно Таблица №1.

4.2 В случае обнаружения ошибки администратор устраняет возникшую ошибку

4.3 В случае недоступности системы резервного копирования резервирование должно осуществляться на вторичный сервер резервного копирования согласно с утвержденной Методики (Таблица №2).

Таблица №1
к Положению по системе резервного копирования данных ИС

Перечень резервируемой информации

№	Наименование данных, оборудования	Наименование резервируемой информации	Периодичность резервного копирования	Тип резервного копирования	Периодичность контроля результатов резервного копирования	Примечание

Таблица №2
к Положению по системе резервного копирования данных ИС

Методика резервного копирования

1. Резервное копирование

1.1 Для организации системы резервного копирования используется клиент-серверное программное обеспечение (далее ПО) Резервное копирование и восстановление файлов в Microsoft Windows.

1.2 С целью оптимизации расходов на развертывание системы резервного копирования, запись резервной копии осуществляется на жесткий диск.

1.3 После контроля резервной копии (в случае безошибочного сохранения) системным администратором осуществляется сброс резервной

копии на перезаписываемый оптический диск высокой плотности хранения данных.

1.4 С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

1.5 Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить во время прогнозируемой минимальной (без учета самого процесса резервирования) нагрузки на место хранения данных, с которого они будут передаваться. Данное время устанавливается системным администратором.

1.6 Существует четыре набора резервных копий:

- суточный набор. Копирование производится в час наименьшей нагрузки каждый день кроме 1 числа месяца и воскресенья (6 томов);

- недельный набор. Копирование производится в час наименьшей нагрузки каждое воскресенье месяца, если оно не совпадает с 1 числом месяца (4 тома);

- месячный набор. Копирование производится в час наименьшей нагрузки 1 числа каждого месяца, если оно не совпадает с 1 января (12 томов);

- годовой набор. Копирование производится 1 января и хранится 3 года.

ИНСТРУКЦИЯ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

Данная Положения регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора по ИБ, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и т.д.), а также общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- пользователь не имеет права сообщать личный пароль никому.

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

В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного сотрудника по информационной безопасности. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. может возникнуть необходимость использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие. Эти сотрудники обязаны сразу же после смены своих паролей передать их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале на хранение

ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при наличии), либо печать уполномоченного представителя отдела обеспечения информационной безопасности.

2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками отдела обеспечения информационной безопасности – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИС.

3. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале.

Повседневный контроль действий исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на ответственного сотрудника по информационной безопасности.

ИНСТРУКЦИЯ ОБ АНТИВИРУСНОЙ ЗАЩИТЕ

1. Основные положения

Задачами антивирусной защиты являются:

- наличие и регламент запуска, а также своевременное обновление систем антивирусной защиты;
- проведение профилактических работ с применением систем антивирусной защиты;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации локальной сети УИТ.

2. Организация работ по антивирусной защите

2.1 Администратор информационной безопасности обеспечивает организацию работ по антивирусной защите.

2.2 В УИТ планированием и проведением мероприятий по антивирусной защите занимаются выделенные для выполнения таких работ специалисты технической службы, администратор по информационной безопасности и системный администратор.

2.3 УИТ должен иметь лицензионные средства антивирусной защиты информации или аттестованные уполномоченными государственными органами другие средства антивирусной защиты.

2.4 В локальной сети УИТ не допускается присутствие и использование программного обеспечения и данных, не связанных с выполнением конкретных функций и задач сотрудников УИТ.

2.5 Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка.

2.6 Отключение или отсутствие обновления антивирусных средств не допускается. Установка и обновление антивирусных средств в УИТ должны контролироваться администратором по информационной безопасности и системным администратором.

2.7 Все мероприятия по антивирусной защите разделяются на индивидуальные и централизованные. Индивидуальные проводятся каждым пользователем самостоятельно, централизованные мероприятия – администратором по информационной безопасности совместно с системным администратором.

2.8 Индивидуальные мероприятия заключаются в проверке операционной системы и её элементов при включении компьютера, а также, при необходимости, и в процессе работы на компьютере. Средства антивирусной защиты должны устанавливаться и обновляться

администратором по информационной безопасности или системным администратором централизованно в соответствии с планом мероприятий, с последующей регистрацией в журналах по установке и обновлению средств антивирусной защиты не реже, чем один раз в месяц. Администратор по информационной безопасности и системный администратор несут ответственность за актуальность антивирусных программ, установленных на рабочих местах.

2.9 Централизованные мероприятия включают профилактические работы по антивирусной защите для серверов локальной сети УИТ, выборочную проверку рабочих станций, плановую проверку архивов, размещенных на внешних носителях.

2.10 Профилактические работы по антивирусной защите серверов общего пользования проводятся администратором по информационной безопасности совместно с системным администратором. Периодичность их проведения должна соответствовать периодичности создания долговременных архивов, но не реже 1 раза в неделю. Обновление базы антивирусных программ на серверах возлагается на системного администратора.

2.11 Плановая проверка архивов, размещенных на внешних носителях, проводится совместно администратором по информационной безопасности и системным администратором, согласно утвержденному графику.

2.12 Выборочная проверка компьютеров проводится администратором по информационной безопасности. Результат проведения выборочной проверки регистрируется в специальном журнале. В случае обнаружения вирусов администратор по информационной безопасности принимает все необходимые меры по ликвидации вирусов, по завершении которых оформляется акт с указанием проведенных работ, утерянной информации и предварительной причины возникновения вируса. Данный акт подписывается пользователем рабочей станции и администратором по информационной безопасности, а также руководителем отдела, за которым закреплена рабочая станция, и руководителем, ответственным за информационную безопасность в УИТ. Руководитель, ответственный за информационную безопасность в УИТ, проводит служебное расследование причин возникновения компьютерного вируса в установленном порядке, по результатам которых должны приниматься соответствующие меры воздействия.

2.13 В случае обнаружения в отделах УИТ компьютерного вируса необходимо представить оперативную информацию о причине возникновения, типе и характеристике вируса.

3. Требования к участникам работ по антивирусной защите

3.1 В должностных инструкциях администратора по информационной безопасности должны быть предусмотрены требования квалификации,

включающие специальные знания по технологии антивирусной защиты и опыт работы с антивирусными средствами защиты информации.

3.2 В должностных инструкциях системного администратора должны быть предусмотрены функции по проведению централизованных мероприятий по антивирусной защите.

4. Ответственность участников работ по антивирусной защите

4.1 В случае нарушения требований данного Положения участники работ по антивирусной защите несут ответственность в соответствии с действующим законодательством и политикой информационной безопасности УИТ.

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ДАННЫХ, МОБИЛЬНЫМИ УСТРОЙСТВАМИ, НАКОПИТЕЛЯМИ ДАННЫХ

1.1 К съемным носителям относятся ленты, диски, флэш-диски, сменные жесткие диски, CD, DVD и печатные носители.

1.2 Необходимо учесть следующие рекомендации по управлению сменными носителями информации:

- если носители информации многократного использования больше не требуются и передаются за пределы УИТ, то их содержимое должно быть уничтожено без возможности восстановления;

- о носителях, выносимых за пределы УИТ, необходимо производить запись в постоянно хранимом регистрационном журнале, а также, где необходимо и целесообразно, нужно применять их авторизацию;

- все носители информации следует хранить в надежном, безопасном месте;

- установка дисководов сменных носителей разрешается только при служебной необходимости.

1.3 При использовании мобильных вычислительных устройств и средств телекоммуникаций, например, ноутбуков, карманных компьютеров, лэптопов, смартфонов и мобильных телефонов, следует соблюдать особую осторожность для предотвращения компрометации деловой информации. Следует соблюдать осторожность при использовании мобильных устройств в общедоступных местах, переговорных комнатах и незащищенных помещениях. Следует внедрить защиту, с целью исключения несанкционированного доступа к мобильным устройствам или раскрытия информации, хранимой и обрабатываемой данными устройствами.

1.4 Мобильные устройства также необходимо физически защищать от краж, не рекомендуется оставлять их без присмотра, например, в автомобилях или другом виде транспорта, гостиничных номерах, конференц-залах.

1.5 На случаи кражи и потери мобильных устройств следует утвердить определенный порядок, принимающий во внимание юридические, страховые и другие требования безопасности УИТ.

1.6 Запрещается подключение USB, Wi-Fi модемов и иных устройств на рабочих станциях без согласования с ответственным сотрудником по ИБ.

ПЕРЕЧЕНЬ РАЗРЕШЕННОГО К ИСПОЛЬЗОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Обновление операционной системы и ее компонентов на рабочих станциях осуществляется ответственными сотрудниками по ИКТ. Требуемый пакет обновлений загружается с сайта производителя ОС и сохраняется на сервере УИТ в специальной папке, после чего распространяется на пользовательские рабочие места. Повторная загрузка пакетов обновления с сайта производителя ОС разрешается в случае повреждения пакета, хранящегося на сервере УИТ. Самостоятельная установка пользователями пакетов обновления операционной системы недопустима.

На всех рабочих станциях и мобильных компьютерах используется ОС Windows, английская версия.

Список прикладных программ, разрешенных к использованию на рабочих станциях.

- *MS Office (OpenOffice)* – работа с текстовыми документами, с электронными таблицами, с презентациями, английская версия.
- *Nod32, Kaspersky* – антивирусный пакет.
- *7-ZIP* – средство работы с электронными архивами.
- *Foxit Reader* – средство просмотра PDF-документов.
- *Mozilla FireFox, Google Chrome* – средство для просмотра WEB страниц.
- *K-Lite Codec Pack* – набор кодеков для видео файлов (по необходимости).
- *Windows Media Player* (только настройка) - программа для воспроизведения звуковых и видео файлов (по необходимости).
- Правовые базы данных Кодекс, Консультант (по необходимости).

Дополнительное программное обеспечение, требуемое для выполнения специализированных задач, устанавливается после согласования с ответственным сотрудником по обеспечению информационной безопасности и с руководством УИТ.

ИНСТРУКЦИЯ ПО РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТОЙ

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. УИТ оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным законодательством и законодательством Республики Узбекистан, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

При работе с ресурсами сети Интернет недопустимо:

- (разглашение информации ограниченного доступа УИТ, ставшей известной сотруднику Организации по служебной необходимости либо иным путем;

- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, имени пользователей, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

При работе с ресурсами Интернет запрещается:

- фальсифицировать свой IP-адрес;
- переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей;

- осуществлять попытки несанкционированного доступа к ресурсам сети, проведение сетевых атак и сетевого взлома и участие в них;

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

- использовать анонимные прокси-серверы;
- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой УИТ.

Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политиками УИТ.

Вся информация о ресурсах, посещаемых сотрудниками УИТ, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также руководству УИТ для детального изучения.

С КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТОЙ

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности и неотделима от нее.

Электронная почта является собственностью УИТ и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам **УИТ** запрещается:

- использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с руководством;
- публиковать свой адрес, либо адреса других сотрудников на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- отправлять сообщения с вложенными файлами, общий объем которых превышает 20 Мегабайт.
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как спам и являются незаконными.
- осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с руководством;
- рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, имени пользователей, пароли и прочие средства для получения несанкционированного доступа к

платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

- распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.

- распространять информацию содержание и направленность, которой запрещены международным законодательством и законодательством Республики Узбекистан включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

- распространять информацию ограниченного доступа;

- предоставлять, кому бы то ни было пароль доступа к своему почтовому ящику.

ПОРЯДОК УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ (АКТИВАМИ) УИТ

1. Общие положения

1.1. Активом является что-либо имеющее ценность для УИТ и следовательно, нуждающееся в защите.

1.2. Системный администратор является ответственным за составление и поддержание в актуальном состоянии Реестра ИР УИТ (далее – Реестр) по форме согласно приложению №13.

1.3. В число ИР (активов) входят базы данных и файлы, резервные копии баз данных и файлов, веб-сайт УИТ и другие.

1.4. В Реестре должна быть установлена и задокументирована классификация ИР (КИ, или открытая информация).

1.5. Необходимо идентифицировать владельцев (структурные подразделения УИТ) всех основных ресурсов (активов) и определить их ответственность за поддержание соответствующих мероприятий по управлению ИБ.

1.6. Владелец ИР (актива) является ответственным за:

- обеспечение соответствующей классификации информации;
- разграничение и периодический пересмотр ограничений и классификации доступа.

1.7. Для каждого ресурса (актива) на основании его ценности следует установить уровень защиты.

1.8. Включается вся необходимая информация, включая описание, формат актива, расположение, ответственного владельца.

2. Классификация информации

2.1. Информацию следует классифицировать, чтобы определить приоритетность, необходимость и степень ее защиты при обращении к ней. Некоторые типы информации могут требовать дополнительного уровня защиты или специальных методов обработки.

2.2. Следует классифицировать информацию по требованиям законодательства, а также по ценности для УИТ.

2.3. Владелец актива является ответственным за классификацию активов, ее периодический пересмотр, а также обеспечение её актуальности и надлежащего уровня.

2.4. Уровень защиты можно оценить с помощью анализа конфиденциальности, целостности, доступности и других требований к информации.

2.5. ИР по категориям доступа разделяются на общедоступные ИР (предназначенные для неограниченного круга пользователей) и ИР с ограниченным доступом (содержащие КИ).

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

2.6. Категории доступности защищаемых ИР:

- «беспрепятственная доступность» (Б) - доступ к ИР должен обеспечиваться в любое время (задержка не должна превышать нескольких секунд или минут);

- «высокая доступность» (В) - доступ к ИР должен осуществляться без существенных временных задержек (задержка не должна превышать нескольких часов);

- «средняя доступность» (С) - доступ к ИР может обеспечиваться с существенными временными задержками (задержка не должна превышать нескольких дней);

- «низкая доступность» (Н) - временные задержки при доступе к ИР практически не лимитированы (допустимая задержка получения результата - несколько недель).

2.7. Категории целостности защищаемой информации:

- «высокая» (В) - ИР, несанкционированная модификация или фальсификация которого может привести к нанесению значительного прямого ущерба, целостность которого должна обеспечиваться гарантированными методами (например, средствами электронной цифровой подписи) в соответствии с обязательными требованиями законодательства;

- «низкая» (Н) - ИР, несанкционированная модификация или фальсификация которого может привести к нанесению незначительного косвенного ущерба, целостность которого должна обеспечиваться методами подсчета контрольных сумм, хеш-функций и т.п.;

- «нет требований» - ИР, к обеспечению целостности которого требований не предъявляется.

3. Маркировка активов

Информационные активы необходимо маркировать. Обычной формой маркировки являются физические метки. Однако некоторые информационные активы как электронные документы нельзя маркировать физически, поэтому необходимо использовать электронные средства маркировки, например уведомляющие метки, которые могут появляться на экранах или дисплеях.

4. Ответственность

Ответственность за обеспечение защиты ИР УИТ, возлагается на ответственного сотрудника по ИБ и системного администратора.

Таблица 1
к порядку управления
информационными
ресурсами (активами) УИТ

РЕЕСТР ИНФОРМАЦИОННЫХ РЕСУРСОВ УИТ

№	Регистрационный номер	Название ресурса	Описание ресурса	Размещение	Использование	Формат	Уровень конфиденциальности	Целостность	Доступность	Частота обновления данных	Владелец
1		Корпоративный брандмауэр FortiNet	Программно-аппаратный комплекс учета трафика и контроля доступа в сеть Интернет	На сервере УИТ (172.16.10.18)	Контроль учета трафика и доступа в Интернет	Цифровой	-			-	УИТ
2		File-сервер DHCP-сервер DNS-сервер		На сервере УИТ (192.168.1.16)		Цифровой	-			До инсталляции нового ПО	УИТ
3		База данных программного продукта 1С	Бухгалтерская информация	На сервере Компании (192.168.1.24)	Работа с бухгалтерскими операциями	*.dbf	ДСП	В	Б	1 день	УИТ
4		Norma		На сервере УИТ (192.168.1.101)		Цифровой	-	-	Б	-	УИТ
5		Резервная база данных программного продукта 1С	Бухгалтерская информация	На сервере УИТ (192.168.1.18)	Работа с бухгалтерскими операциями	*.dbf	ДСП	В	Б	1 день	УИТ
6		Сайт Компании	https://www.inha.uz/	Сайт УИТ		*hml *jpg *bmp *png *txt	н/с			По мере необходимости	УИТ

¹Уровень Конфиденциальности: ДСП и н/с;

²Целостность: В, Н – (нет требований);

³Доступность: Б, В, С, Н;

⁴Пользователи: ФИО персонала, которому санкционирована работа с ресурсом на основе матрицы доступа;

⁵Владелец: ФИО персонала, ответственного за информационный ресурс

Приложение 10

ЖУРНАЛ РАБОТЫ ЛОКАЛЬНОЙ СЕТИ УИТ

№	Дата	Событие	Примечание

**ЖУРНАЛ УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ, ФАКТОВ ВСКРЫТИЯ И
ОПЕЧАТЫВАНИЯ РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ, ВЫПОЛНЕНИЯ
ПРОФИЛАКТИЧЕСКИХ РАБОТ, УСТАНОВКИ И МОДИФИКАЦИИ АППАРАТНЫХ
И ПРОГРАММНЫХ СРЕДСТВ**

№	Дата	Событие	Примечание

**ЖУРНАЛ ОЗНАКОМЛЕНИЯ С ПОЛИТИКОЙ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ В УИТ**

№	Ф.И.О.	Должность	Подразделение	Дата	Подпись