УТВЕРЖДЕН
приказом Архивной службы КБР
от 19 марта 2018 года № 24

РЕГЛАМЕНТ
эксплуатации информационно-вычислительной сети Архивной службы Кабардино-Балкарской Республики

1. Введение

Информационно-вычислительная сеть (далее ИВС) Архивной службы Кабардино-Балкарской Республики интегрируется в единую защищенную сеть передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления.

Настоящий Регламент определяет основные правила построения, функционирования и развития ИВС. Исполнение Регламента обеспечит надежную, безопасную и эффективную работу ИВС.

Соблюдение Регламента отвечает интересам всех пользователей ИВС.

В Регламенте используются следующие понятия, определенные в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

информация - сведения (сообщения, данные) независимо от формы их представления;

документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

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

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

В Регламенте использованы также следующие основные понятия и термины:

информационные ресурсы (ИР) – отдельные документы и отдельные массивы документов, документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах);

средства обеспечения информационных систем и технологий – программные, технические, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их функционирование;

пользователь информационной системы - субъект, обращающийся к информационной системе за получением необходимой ему информации и пользующийся ею.

вычислительная сеть - аппаратная основа информационно-телекоммуникационной сети, совокупность вычислительных машин (персональных компьютеров, специализированных компьютеров, серверов), периферийных устройств (принтеров, сканеров, плоттеров, видеокамер и др.), специализированных сетевых устройств (концентраторов, коммутаторов, маршрутизаторов, точек доступа радиосети), кабельной системы;

сервер - специализированная вычислительная машина, предоставляющая пользователям разделяемые ресурсы, или специальное программное обеспечение, под управлением которого вычислительная машина предоставляет пользователям доступ к разделяемым ресурсам и сетевым сервисам;

разделяемые ресурсы - периферийные устройства, дисковое пространство, вычислительная мощность центрального процессора;

сетевые сервисы – специальные процессы сетевых операционных систем, обеспечивающие взаимодействие компьютеров между собой, а также с другим активным сетевым оборудованием в TCP/IP-сетях (DNS, HTTP, FTP, DHCP и т.п.);

ресурсы вычислительной сети - разделяемые ресурсы подключенных к ней компьютеров, пропускная способность сети, внешние каналы связи, к которым подключена сеть;

сетевые информационные ресурсы - информация, к которой пользователи могут получать доступ, используя компьютеры, подключенные к вычислительной сети;

доступ к сети - возможность использовать ресурсы сети;

аутентификация - определение индивидуальных признаков по регистрационному имени, сетевому адресу, паролю;

авторизация - определение возможности предоставить доступ к сетевому ресурсу на основе результата аутентификации;

сеть общего пользования - информационно-телекоммуникационная сеть, доступ к которой должен предоставляться ее владельцем всем желающим на основании договора в соответствии с лицензией владельца на предоставление услуг связи;

корпоративная сеть - вычислительная сеть, не предназначенная для общего использования, доступ к которой ограничен владельцем;

Internet - глобальная информационно-телекоммуникационная сеть, объединяющая сети общего пользования и корпоративные сети;

RSNet - российский государственный сегмент сети RSNet;

защищенная сеть - корпоративный сегмент сети, реализованный по технологии VipNet заключающийся в шифровании информации при передаче по общедоступным каналам связи;

НСД - не санкционированный доступ к информации;

СЗИ - средства защиты информации.

2. Организационно-правовые основы функционирования ИВС

Функционирование сети осуществляется в соответствии с законами РФ и постановлениями Правительства КБР:

- «Гражданский кодекс РФ»;
- «О безопасности» от 05.03.1992 г. № 2446-1;
- «О государственной тайне», от 21.07.1993 г. № 5485-1;
- «О связи», от 07.03.2011 г. № 26-ФЗ;
- «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 149-ФЗ;
- «Об оперативно-розыскной деятельности», от 12.08.1995 г. № 144-ФЗ;
- «О единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления», постановление Правительства КБР от 08.07.2016 г. № 126-ПП;

3. Состав и структура информационно-вычислительной сети

3.1. Структурированная кабельная сеть

ИВС объединяет между собой компьютеры на рабочих местах работников, серверы, сетевые устройства. Аппаратной основой ИВС является кабельная система сети.

Структурированная кабельная сеть - это единый технологический объект, предназначенный для организации связи в помещениях и между отдельными сооружениями. В состав специального оборудования кабельной системы входят:

- точки подключения к сети на рабочих местах (информационные и телефонные розетки);
- горизонтальная кабельная проводка от розеток на рабочих местах до узлов промежуточной коммутации;
- узлы промежуточной коммутации (промежуточные кроссы);

- магистральная (вертикальная) кабельная проводка от точек промежуточной коммутации до центрального узла коммутации;

- центральный узел коммутации (телекоммуникационный узел) и центральный кросс (специальное оборудование коммутации кабелей).

- розетки 220 В (для подключения оргтехники).

Точка подключения. В точках подключения к кабельной системе присоединяются компьютеры, телефонные аппараты, периферийные устройства и прочее оборудование.

Узел коммутации. В узлах коммутации к кабельной системе присоединяются активные сетевые устройства - коммутаторы и маршрутизаторы (обеспечивают возможность передачи данных между компьютерами в сети) и телефонные IP станции (обеспечивают внутреннюю телефонную связь).

В точке присутствия телефонной компании (кабельный кросс) к структурированной кабельной сети подключаются линии телефонной сети общего пользования (городские телефонные линии).

3.2. Подключение компьютеров к сети

В соответствии с организационной структурой территориально распределенные точки подключения к сети в помещениях группируются в локальные сети (виртуальные локальные сети, VLAN). Каждая точка подключения относится к определенной VLAN. Виртуальная локальная сеть формируется управляемым коммутатором доступа на промежуточном узле коммутации.

Коммутаторы доступа связаны между собой через центральный коммутационный узел (центральный коммутатор).

В ИВС не могут использоваться точки беспроводного доступа к сети.

Работы по организации, учету и объединению виртуальных локальных сетей выполняются централизованно техническим администратором.

3.3. Адресация компьютеров в сети

В ИВС используются физические (MAC) адреса и система IP-адресов. Каждый подключенный к сети компьютер получает фиксированный IP-адрес, связанный с физическим (MAC) адресом сетевого интерфейса компьютера. Для каждого подключенного к сети компьютера задается IP-адрес маршрутизатора (адрес шлюза по умолчанию), через который он может связываться с компьютерами в других локальных сетях и Интернет. Для каждого компьютера задается маска подсети, к которой принадлежит его IP-адрес. Каждой локальной сети (VLAN) соответствует своя подсеть IP-адресов.

Ведется учет всех компьютеров, подключаемых к ИВС, по их физическим адресам. Запрещено подключение незарегистрированных компьютеров к ИВС и произвольное присвоение им IP-адресов сотрудниками подразделений.

3.4. Система управления сетевыми компьютерами и пользователями

Запрещено использование компьютеров с нелицензионными экземплярами операционной системы.

Учет лицензий, управление лицензиями, установку лицензионного программного обеспечения рабочих станций выполняет отдел правового и

информационного обеспечения, контроля за исполнением архивного законодательства Архивной службы КБР (далее - ОПИОКИАЗ).

Для управления учетными записями пользователей, разграничения прав доступа к ресурсам компьютеров и управления операционными системами и программным обеспечением в ИВС используется доменная система Microsoft Active Directory.

Каждый компьютер, присоединенный к ИВС, регистрируется в одном из доменов в зависимости от его функционального назначения.

Каждый пользователь ИВС для использования информационных ресурсов регистрируется и получает доступ к сетевым ресурсам после аутентификации и авторизации. Запрещен неавторизованный доступ к сетевым ресурсам.

3.5. Соединение ИВС с RSNet

ИВС подключается к сети RSNet с использованием услуг оператора ФСО России. Все подключения ИВС к другим сетям производятся в телекоммуникационном узле ИВС.

3.6. Состав ИВС

В состав ИВС входят:

- телекоммуникационный узел;
- административно-технический сетевой сегмент;
- локальные вычислительные сети подразделений (ЛВС);
- отдельные персональные компьютеры подразделений, не имеющих выделенных ЛВС;
- персональные компьютеры индивидуальных абонентов сети;
- магистраль, обеспечивающая межсетевые соединения.

3.7. Прочие компьютеры и ЛВС

Правила настоящего регламента не распространяются на компьютеры и локальные вычислительные сети подразделений, не имеющие защищенного соединения с магистралью ИВС.

Должны исполняться следующие требования, ответственность за соблюдение которых лежит на пользователях автоматизированного рабочего места:

- использовать только программное обеспечение, на которое имеются приобретенные лицензии или свободно-распространяемое программное обеспечение с лицензиями на неограниченное (свободное) использование;
- подключаться к сетям других организаций или Internet только на основании письменного разрешения руководителя Архивной службы КБР.

4. Назначение и использование ИВС

ИВС создается и развивается для решения следующих основных задач:

- обеспечение рабочего процесса;
- обеспечение процесса управления;
- обеспечение защищенной IP телефонией.

Использование ИВС в других целях запрещается.

4.1. Обеспечение процесса управления

Для обеспечения процесса управления используются компьютерные сети в подразделениях. Персональные компьютеры и сетевые ресурсы, включая доступ к сети RSNet, должны использоваться сотрудниками только для выполнения ими своих обязанностей в соответствии с должностными инструкциями.

Все компьютеры, подключенные к сети и используемые для обеспечения процесса управления, относятся к определенному, централизованно управляемому домену. Все сотрудники, которым необходимо в связи с их должностными обязанностями использовать сетевые ресурсы, должны быть зарегистрированы в этом домене, иметь индивидуальное имя пользователя (логин) и пароль доступа. Каждый пользователь должен регистрироваться для работы в сети под своим именем.

Запрещено передавать индивидуальный логин и пароль доступа другому лицу.

Запрещено использование ресурсов ИВС анонимными пользователями, однозначная аутентификация которых невозможна.

Запрещается любое коммерческое (с целью извлечения личной материальной выгоды) использование сетевых ресурсов ИВС.

5. Управление сетью и организация эксплуатации сети

5.1. Управление сетью

Управление сетью включает в себя реализацию следующих основных функций:

- планирование, создание и сопровождение кабельной системы ИВС;
- организация и сопровождение системы локальных сетей (VLAN), коммутаторов уровня доступа, магистральных коммутаторов и маршрутизаторов ИВС;
- составление и поддержка адресного плана, взаимодействие с регистром IP-адресов, поддержка службы автоматического выделения адресов (DHCP) ИВС, регистрация компьютеров в службе DHCP;
- организация и сопровождение внешних каналов связи, внешней маршрутизации ИВС, связи с сетями органов государственной власти и органов местного самоуправления КБР RSNet;
- взаимодействие с операторами связи и сетевыми управляющими центрами других организаций для организации межсетевой связи;
- организация и поддержка доменной службы имен, сопровождение домена и зоны HGKBR.RU;
- организация и поддержка доменов службы каталогов ИВС, регистрация объектов доменов и сопровождение их учетных записей;
- организация и поддержка службы корпоративной электронной почты в зоне kbr.ru, регистрация абонентов и сопровождение их учетных записей;
- организация и поддержка системы внутренней телефонной связи по IP-сети (VoIP), регистрация абонентов голосовых служб и сопровождение их учетных записей;

- установка и поддержка лицензионного программного обеспечения на компьютерах, подключенных к ИВС и учёт использования лицензий в ИВС, организация и поддержка доступа к сетевым лицензионным ключам;

- организация и поддержка сетевых информационных ресурсов в форме файловых серверов, web-серверов, серверов баз данных и др.;

- разработка и реализация мероприятий по защите ресурсов ИВС от несанкционированного доступа;

- обеспечение резервного копирования и восстановления информационных ресурсов и информационных ресурсов подразделений по их запросам;

5.2. Эксплуатация сети

Процесс эксплуатации должен обеспечивать реализацию всех этапов жизненного цикла компонентов ИВС:

- формирование запроса на создание объекта (пользователь, сотрудник);

- установка операционной системы и необходимых для выполнения функциональных обязанностей программных продуктов;

- регистрация в службе каталогов;

- установка антивирусной защиты;

- установка средств защиты от НСД DallasLock версии К;

- установка программного комплекса ViPNet Client предназначенного для защиты рабочих мест корпоративных пользователей;

- сопровождение функционирования объекта, модернизация;

- регистрация в информационных системах (ГИС ЕСЭД КБР);

- модернизация или вывода объекта из эксплуатации;

- списание объекта и утилизация.

В случаях, когда кабельные системы и другие программно-аппаратные компоненты ИВС находятся в ведении подразделений, руководители подразделений должны согласовать порядок разделения ответственности и уровень предоставления сервиса со стороны. При этом должны быть оговорены следующие вопросы разделения ответственности:

- обязательство подразделения соблюдать регламент ИВС;

- точка разграничения ответственности (как правило, в месте присоединения оборудования или сети подразделения к ИВС);

- список сетевых сервисов, используемых в подразделении, за организацию и сопровождение которых несет ответственность подразделение;

- разграничение ответственности отделов, предоставляющих сервисы и подразделения на этапах жизненного цикла кабельных систем, сетевых устройств, программного обеспечения, сетевых сервисов в сети или на устройствах подразделения;

- меры по обеспечению безопасности сети;

- сотрудники подразделения, отвечающие за эксплуатацию сети или устройств, используемых в подразделении.

6. Безопасность

6.1. Мероприятия по защите сети

Соблюдение законодательства и рекомендации регуляторов в области защиты информации (ФСБ России, ФСТЭК России) в области организации информационных процессов в сетях общего пользования, включая ограничения на распространение информации, возлагается на руководителей подразделений, которые эксплуатируют средства вычислительной техники (СВТ).

Запрещено подключать к ИВС локальные сети и оборудование, на которых производится обработка информации со степенью секретности «Для служебного пользования», «Секретно» и выше. Ответственность за выполнение этого требования возлагается на руководителей подразделений, использующих в своей работе компьютеры, подключенные к ИВС.

Защита ИВС от несанкционированного доступа обеспечивается администратором безопасности, совместно с лицами, ответственными за СВТ в подразделениях, путем реализации организационных и технических мероприятий.

Организационные мероприятия включают в себя:

- постоянный контроль соблюдения настоящего регламента;
- не допускать к автоматизированному рабочему месту лиц, не являющихся работниками соответствующего структурного подразделения;
- ограничение доступа сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование ИВС, к магистральным коммутаторам;
- контроль состава и структуры сети и пресечение несанкционированного подключения СВТ к ИВС.

Технические мероприятия включают в себя:

- регулярную смену сетевых паролей;
- обеспечение защиты настроек базовой системы ввода-вывода;
- обеспечение межсетевого экранирования;
- физическое выделение сегментов сети, организация межсетевых экранов для разделения локальных сетей ИВС и защиты от несанкционированного доступа (НСД) из внешних сетей;
- отслеживание запуска и пресечение использования программного обеспечения, затрудняющего или нарушающего нормальную работоспособность сети, компьютеров в ней и нарушающего безопасность сети;
- регистрацию пользователей на сервере безопасности DallasLock;
- фильтрация сетевых протоколов на маршрутизаторах в соответствии с применяемой политикой безопасности;
- организация централизованной антивирусной защиты всех компьютеров, подключенных к ИВС, с использованием административного сервера и агентов на каждом компьютере;
- защита от несанкционированной массовой рассылки по электронной почте, пресечение несанкционированной массовой рассылки через почтовые серверы;
- контроль и ограничение трафика в каналах связи ИВС с другими сетями и Internet с целью предотвращения нецелевого использования ресурсов внешних каналов связи.

ОПИОКИАЗ проводит политику максимального использования на компьютерах в ИВС программного обеспечения, обеспечивающего авторизацию доступа к консоли компьютера и к сетевым сервисам и централизованную аутентификацию пользователей, получивших доступ в сеть.

6.2. Возможные злоупотребления и защита от них

К злоупотреблениям, в первую очередь, относится деятельность, нарушающая действующее законодательство (гражданское и уголовное).

К злоупотреблениям относится также:

- использование ИВС в коммерческих целях;
- организация точек доступа к ИВС по беспроводным, коммутируемым, выделенным и физическим линиям без согласования с руководством;
- использование отчуждаемых (USB, ESATA и т.д.) носителей и запись на CD диски без регистрации в журнале и без согласования с руководством;
- незапланированная и необоснованная производственной необходимостью загрузка сети.

В случае злоупотребления при использовании сетевых сервисов нарушители частично или полностью отстраняются от пользования сетью и несут ответственность в соответствии с действующим законодательством РФ.

7. Развитие ИВС

7.1. Способы присоединения оборудования к ИВС

Подключение компьютерного оборудования и периферийных устройств к ИВС производится одним из трех способов:

- через коммутаторы доступа в промежуточных коммутационных точках; этот способ присоединения применяется для ЛВС подразделений;
- магистральные устройства ИВС в центральной точке коммутации;
- через сети операторов связи с использованием VPN; этот способ присоединения применяется для территориально удаленных подразделений, имеющих соединение по сети Internet, при подключении IP телефонного аппарата.

7.2. Планирование развития сети

Планирование развития ИВС проводится по следующим направлениям:

- расширение и модернизация кабельной системы области доступа к сети, включая коммутационное оборудование на промежуточных кроссах (в точках промежуточной коммутации), планирование вывода из эксплуатации устаревших элементов кабельной системы;
- расширение и модернизация вертикальной кабельной системы (магистральной кабельной системы), планирование вывода из эксплуатации устаревших элементов кабельной системы;
- модернизация центрального узла коммутации;
- развитие корпоративной сети, объединяющей филиалы, обеспечивающей доступ к другим ведомственным сетям;
- развитие системы защиты сети;
- развитие внешней связности сети;

- развитие сервисной инфраструктуры ИВС, модернизация серверной базы, планирование вывода из эксплуатации устаревшего оборудования;

- поддержка и расширение пакета лицензионного программного обеспечения для сетевого применения.
