|  |  |
| --- | --- |
|  | Приложение 8 к приказу комитета по культуре города Барнаула от 29 июля 2021г. №64 |

ПОРЯДОК

обеспечения защиты информационных ресурсов при удаленном доступе через сеть

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АП – абонентский пункт.

КИ – конфиденциальная информация.

ЛВС – локальная вычислительная сеть.

ИС – информационная система.

ГИС – государственная информационная система.

ИСПДн – информационная система персональных данных.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения

1.1. Порядок обеспечения защиты информационных ресурсов при удаленном доступе через сеть (далее – Порядок) разработан с целью регламентации обеспечения защиты информации в ГИС, ИСПДн, ИС, содержащих другие виды КИ, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к объектам критической информационной структуры (далее – ИС) комитета по культуре города Барнаула (далее –комитет) при удаленном доступе к АП через сеть.

2. Сетевые сервисы.

2.1. Сервис – совокупность аппаратных и программных средств, обеспечивающих выполнение функций, направленных на предоставление информационных услуг, информационных или вычислительных ресурсов или обеспечение работоспособности других сервисов.

2.2. Политика в области определения списка сервисов, поддерживаемых в корпоративной сети, выбора технических и программных средств их реализации и прочие вопросы, связанные с созданием, поддержкой, развитием и закрытием сервиса целиком определяется ответственными за функционирование ЛВС, подразделением по защите информации, либо АИБом.

2.3. Сервис в сети комитета может быть создан по согласованию с ответственными за функционирование ЛВС, подразделением по защите информации, либо АИБом и председателем комитета.

2.4. Сотрудникам запрещается создавать на включенных в корпоративную сеть компьютерах и серверах сервис, доступный для внешних пользователей или из внешних сетей без согласования с ответственными за функционирование ЛВС, подразделением по защите информации либо АИБом и председателем комитета.

2.5. Каждый создаваемый сервис должен иметь администратора, ответственного за его поддержку и эксплуатацию.

2.6. ИС обязан выполнять все распоряжения и учитывать рекомендации ответственных за функционирование ЛВС и подразделения по защите информации, либо АИБа.

2.7. Администратор общедоступного сервиса определяет порядок его использования, разрабатывает и своевременно обновляет инструкции и другую необходимую документацию для пользователей данного сервиса.

2.8. При обнаружении общедоступного сервиса, не имеющего данных об администраторе и не зарегистрированном ответственными за функционирование ЛВС и подразделением по защите информации (либо ответственным за обеспечение защиты информации), они принимают меры по ликвидации такого сервиса.

2.9. Любые действия, связанные с поддержанием работоспособности ЛВС, ее модернизацию или иное изменение, создание новых и удаление старых сервиса вправе производить только администратор ИС либо ответственный за функционирование ЛВС.

3.Удаленный доступ

3.1. Запрещается устанавливать сервера удаленного доступа и сетевые сервисы, доступные за пределами ЛВС комитета без письменного согласования с ответственным за функционирование ЛВС, подразделением по защите информации либо АИБом и председателем комитета.

3.2. Запрещается получать через сеть Интернет доступ к информации, располагающейся на рабочих станциях и серверах комитета, с ограниченным доступом.

3.3. Сервер удаленного доступа считается рабочей станцией общего доступа, администратор сервера несет ответственность за сервер удаленного доступа и за всех пользователей работающих на сервере.

3.4. Администраторы серверов удаленного доступа обязаны по требованию сотрудников подразделения по защите информации (либо ответственного за обеспечение защиты информации) представлять список лиц, получающих доступ с указанием времени сеансов удаленного доступа для каждого лица.

3.5. Запрещается предоставление и использование услуг удаленного доступа без принятых технических мер по обеспечению невозможности доступа в ЛВС комитета через сервер удаленного доступа.

3.6. Запрещается организация доступа к серверам и рабочим станциям комитета по всем протоколам удаленного доступа из внешних сетей.

4. Порядок предоставления внешних и внутренних IP адресов

4.1. Предоставление внешних IP-адресов осуществляется на основе официальных письменных заявок. В заявке должны быть указаны:

назначение получаемого внешнего IP адреса;

сетевые сервисы, предполагаемые к функционированию на оборудовании, на котором будет использоваться полученный внешний IP адрес;

ответственный за функционирование сетевых сервисов;

ответственный за техническую поддержку сервисов.

4.2. Решение о предоставлении внешних IP-адресов принимает председатель комитета.

4.3. Внутренние IP-адреса предоставляются по заявкам.

4.4. Заявки рассматриваются в индивидуальном порядке и могут быть отклонены. Как внешние, так и внутренние IP адреса могут быть отключены или отозваны в случае обнаружения связанных с ними злоупотреблений или нарушений на установленный период или до устранения причин, повлекших за собой отключение IP адреса.

5.Работа с электронной почтой

5.1. Заявки на регистрацию адреса электронной почты, изменение регистрационных данных или пароля, принимаются только от заместителей председателя комитета.

5.2. Отправка электронной почты разрешается только через почтовые сервера комитета.

5.3. Запрещается отправка электронной почты от чужого имени.

6. Работа в сети Интернет

6.1. Запрещается работа в сети Интернет для неавторизованных сотрудников.

6.2. Запрещается использование сети Интернет в личных и коммерческих целях.

6.3. Выход в сеть Интернет разрешен круглосуточно.

7. Нарушение правил работы в Интернет

7.1.Перечень нарушений правил работы в сети Интернет:

установка имен рабочей станции или домена, не удовлетворяющих принятым правилам наименования рабочих станций, доменов и рабочих групп;

обход учетных систем получаемого трафика, их повреждение или дезинформация;

преднамеренная рассылка вирусов через сеть Интернет;

предоставление служебной информации для общего доступа;

распространение через сеть Интернет информации, запрещенной действующим законодательством или не соответствующей морально-этическим нормам ее получателей, а также рассылка обманных, беспокоящих или угрожающих сообщений и рассылка незапрашиваемых сообщений (спама) за исключением служебных сообщений;

установка и/или удаление программного обеспечения без согласования с ответственными за функционирование ЛВС.

8. Публикация служебной информации

8.1. Запрещается публиковать для всеобщего доступа детальную служебную информацию, касающуюся устройства и архитектуры ЛВС, в т. ч. схемы ЛВС и ее сегментов, точек подключения, информацию о назначенных рабочим станциям IP адресах и именах, используемых на серверах, средствах удаленного доступа и т. п., а также информацию о других получателях без их личного согласия и разрешения руководства.

9. Ответственность

9.1. Контроль за соблюдением Порядка возлагается на ответственных за функционирование ЛВС, подразделение по защите информации (либо ответственного за обеспечение защиты информации). В случае выявления нарушений и злоупотреблений могут быть применены нижеуказанные меры на установленный период или до устранения причин, повлекших за собой принятие мер:

9.1.1. Персонально к нарушителю:

отключение доступа в сеть Интернет;

лишение возможности работы за компьютером;

ограничение доступа к информационным ресурсам сети Интернет;

ограничение на использование электронной почты;

принятие административных мер воздействия.

9.1.1. К рабочей станции или серверу:

отключение доступа в сеть Интернет;

отключение возможности работы в локальной сети;

физическое отключение от ЛВС;

удаление информации из общего доступа.