|  |  |
| --- | --- |
|  | Приложение 20 к приказу комитета по культуре города Барнаула  от 29 июля 2021г. №64 |

РЕГЛАМЕНТ

по работе пользователей в информационных системах

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

ИС – информационная система.

ГИС – государственная информационная система.

ИСПДн – информационная система персональных данных.

КИ – конфиденциальная информация.

ЛВС – локальная вычислительная сеть.

НСД – несанкционированный доступ.

ПДн – персональные данные.

ПО – программное обеспечение.

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.

Допуск пользователей для работы в ИС, в том числе ИСПДн – выполнение обладателем информации или другими уполномоченными должностными лицами определенных процедур, связанных с оформлением права лица на доступ к защищаемой информации.

Доступ пользователей для работы в ИС, в том числе ИСПДн – получение каждым пользователем ИС, в том числе ИСПДн, только письменного разрешения обладателя информации или другого уполномоченного должностного лица на право работы с информацией с учетом его служебных обязанностей.

1. Общие положения

1.1. Регламент по работе пользователей в информационных системах (далее – Регламент) разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» и других действующих нормативно-правовых актов Российской Федерации.

1.2. Регламент определяет общие требования к организации допуска пользователей для работы в ИС общего пользования, ГИС, ИСПДн, ИС, содержащих другие виды КИ, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к ключевым системах информационной инфраструктуры (далее – ИС) комитета по культуре города Барнаула (далее –комитет) при обработке (наборе, редактировании и печати) защищаемых информационных ресурсов, права и обязанности пользователей при работе в защищаемой ИС, в том числе ИСПДн, ответственность за невыполнение предъявляемых к работе пользователей требований.

1.3. Основная цель обеспечения информационной безопасности – предотвращение несанкционированного, в том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение, а также иные несанкционированные действия.

1.4. Методическое руководство работой пользователей, настройку параметров средств защиты, контроль работоспособности и соответствия установленным требованиям параметров настройки средств защиты, установленных на персональных компьютерах, осуществляет ответственные за обеспечение защиты информации в ИС.

1.5. Ответственность за безопасность информации и соблюдение установленных правил работы при ее обработке возлагается на лиц, допущенных к их обработке.

2. Порядок организации допуска пользователей для работы в ИС

2.1. Порядок допуска определяется в соответствии с Положением о разрешительной системе допуска.

3. Общие принципы работы пользователя

3.1. Работа пользователей в системе разрешена только на закреплённых за ними компьютерами, в определенное время и только с разрешенными программами и сетевыми ресурсами.

3.2. Вход в систему в обязательном порядке осуществляется на основе ввода (по запросу системы) имени, присвоенного при первичной регистрации администратором ИС, и ввода личного пароля, требования к которому установлены в «Инструкции по организации парольной защиты комитета по культуре города Барнаула». Ни при каких условиях пароль не может быть сообщён другому лицу за исключением случаев, предусмотренных в «Инструкции по организации парольной защиты комитета по культуре города Барнаула». В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к АИБу.

Все автоматизированные рабочие места, установленные в комитете, имеют унифицированный набор установленного программного обеспечения, определенный в «Перечне, разрешенного к использованию в комитете по культуре города Барнаула программного обеспечения». Самостоятельная установка программного обеспечения на автоматизированные рабочие места запрещена. Установка и удаление любого программного обеспечения производится только уполномоченными сотрудниками в порядке, установленном в комитете. Установка и использование игровых программ запрещено.

3.3. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется уполномоченными сотрудниками. Самовольное перемещение средств вычислительной техники является нарушением персональной ответственности за сохранность переданных сотруднику во временное пользование средств автоматизации. Перемещение любых средств вычислительной техники производится в порядке, установленном в комитете по культуре города Барнаула. Изменение конструкции, конфигурации средств вычислительной техники запрещено.

3.4. Для постоянного хранения и обработки защищаемых информационных ресурсов разрешается использовать исключительно каталоги, определенные АИБом или администратором ИС. Использование отчуждаемых носителей в данных целях запрещено.

3.5. Пользователю разрешается обрабатывать информацию в рамках определенных полномочий доступа, обрабатывать информацию с грифом конфиденциальности выше заявленного при регистрации запрещено.

3.6. Пользователю запрещается осуществлять попытки НСД к ресурсам системы и других пользователей; пытаться подменять функции АИБа по перераспределению времени работы и полномочий доступа к ресурсам компьютера.

3.7. При обнаружении неисправности в работе автоматизированного рабочего места (АРМ), элементов информационной системы, средств защиты пользователю запрещается продолжать работать на АРМ. Об обнаруженных неисправностях необходимо сообщить АИБу или администратору ИС.

4. Обеспечение безопасности персональных данных при использовании сети Интернет

4.1. Доступ к сети Интернет предоставляется в соответствии с должностными обязанностями сотрудника с целью получения оперативной и достоверной информации, необходимой для выполнения должностных обязанностей. Разрешение и изменение доступа к ресурсам Интернет (в том числе к внешним почтовым сервисам) производится в порядке, установленном в комитете.

4.2. Пользователям, имеющим право доступа в Интернет запрещается:

пересылка документов, содержащих защищаемые информационные ресурсы по сети Интернет, электронной почте или с использованием клиентов службы мгновенного обмена сообщениями (ICQ, jabber и т. п.);

использование сети Интернет для развлечения, в т. ч. посещения сайтов «социальных сетей» и сервисов, и получения информации, не относящейся к функциональным обязанностям пользователя;

доступ к сети Интернет и электронной почте не со своего рабочего места с использованием данных своей учетной записи;

предоставление доступа к сети Интернет с использованием данных своей учетной записи другим лицам;

публикация своего адреса электронной почты в электронных каталогах и на поисковых машинах сети Интернет;

подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т. п., не связанные с выполнением пользователем функциональных обязанностей;

открытие (запуск на выполнение) файла, полученного из сети Интернет или по электронной почте, без предварительной проверки его антивирусным ПО.

5. Порядок проведения антивирусного контроля

5.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по электронной почте, интернет-ресурсам, а также информация на съемных носителях (флешках, CD-ROM и т. п.).

5.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.), либо на наличие заражения съемного носителя, пользователь самостоятельно или вместе с АИБом должен провести внеочередной антивирусный контроль своей рабочей станции.

5.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

приостановить работу;

поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в комитете;

провести лечение или уничтожение зараженных файлов.

Пользователям запрещается:

отключать средства антивирусной защиты информации во время работы;

открывать сомнительные электронные письма (необходимо удаление), ссылки, сайты, источники переноса информации.

6. Обеспечение безопасности защищаемой информации при использовании съемных носителей

6.1. Пользователям запрещается:

хранить съемные носители с защищаемой информацией вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить съемные носители с защищаемой информацией из служебных помещений для работы с ними на дому.

6.2. При отправке или передаче защищаемой информации, адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка защищаемой информации адресатам на съемных носителях осуществляется в установленном порядке.

7. Обеспечение безопасности перед началом обработки защищаемой информации

7.1. Перед началом обработки защищаемой, необходимо убедиться в том, что:

в помещении, в котором ведется работа защищаемой информацией, отсутствуют посторонние лица;

технические средства, с использованием которых осуществляется обработка защищаемой информации, находятся в исправном состоянии;

используемые в работе носители защищаемой информации, не повреждены;

к защищаемой информации не был осуществлен НСД.

8. Обеспечение безопасности во время обработки защищаемой информации

8.1. Во время обработки защищаемой информации необходимо обеспечить:

недопущение нахождения в помещении, в котором ведется работа, посторонних лиц;

недопущение воздействия на технические средства, с использованием которых осуществляется обработка, способного нарушить их функционирование;

постоянный контроль за соблюдением условий эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией;

недопущение несанкционированного доступа к информации.

8.2. Во избежание получения НСД к информационным ресурсам АРМ сотрудника устанавливается хранитель экрана, который автоматически включается через 10 минут отсутствия работы на данном компьютере, при этом выход из режима хранителя экрана возможен только при введении идентификационных данных пользователя. При необходимости отлучиться от рабочего места пользователь обязан принудительно запустить хранитель экрана посредством комбинации клавиш «Windows + L» либо другим доступным способом.

9. Обеспечение безопасности при завершении обработки защищаемой информации

9.1. После завершения сеанса обработки защищаемой информации необходимо обеспечить:

исключение возможности несанкционированного проникновения или нахождения посторонних лиц в помещении, в котором размещены технические средства, используемые для обработки;

работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке защищаемой информации.

10. Порядок действий в случае обнаружения фактов нарушения безопасности защищаемой информации

10.1. При нарушении порядка предоставления защищаемой информации, пользователям информационной системы необходимо приостановить их предоставление.

10.2. При обнаружении НСД к защищаемой информации необходимо немедленно прекратить несанкционированный доступ.

10.3. При модификации или уничтожении защищаемой информации, вследствие НСД к ним необходимо обеспечить их незамедлительное восстановление.

10.4. В случае обнаружения фактов несоблюдения условий хранения носителей защищаемой информации, использования средств защиты информации, которые могут привести к нарушению конфиденциальности защищаемой информации, или другим нарушениям, приводящим к снижению уровня защищенности защищаемой информации, необходимо произвести фиксацию данных фактов, служебное расследование и заключение по данным фактам, разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

10.5. Обо всех случаях нарушения безопасности защищаемой информации необходимо немедленно поставить в известность АИБа и произвести служебное расследование.

11. Права пользователей

11.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИС, присвоенными АИБом данному пользователю. При этом для хранения файлов, содержащих защищаемую информацию, разрешается использовать только специально выделенные каталоги, а также соответствующим образом учтенные внешние носители.

12. Ответственность пользователей

12.1. Пользователь отвечает за правильность включения и выключения АРМ, входа в систему и все действия при работе в ИС.

12.2.Пользователь ИС, несет персональную ответственность за соблюдение установленных требований во время работы в ЛВС.

12.3. Пользователи ИС, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами комитета.

12.4. Ответственность за допуск пользователя к ЛВС и установленные ему полномочия несет АИБ.

13. Заключительные положения

13.1. Проверка и пересмотр настоящей Инструкции осуществляются в следующих случаях:

при пересмотре межотраслевых и отраслевых требований обеспечения безопасности информации;

при внедрении новой техники и (или) технологий;

по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности информации;

по требованию представителей органов контроля в сфере обеспечения безопасности информации.

13.2. По всем возникающим вопросам при работе в ИС, необходимо обращаться к АИБу.