**Проект**

**Распоряжение**

**об организации и выполнении мероприятий по защите информации в *ОРГАНИЗАЦИИ***

На основании федеральных законов от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации» и от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», приказов ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования», «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утверждённых приказом председателя Гостехкомиссии России от 30 августа 2002 г. № 282, других нормативных правовых актов Российской Федерации, нормативных и методических документов в области защиты информации, для организации и выполнения мероприятий по защите информации в *ОРГАНИЗАЦИИ*:

1. Назначить *указать должность и ФИО* ответственным за защиту информации.

2. Назначить *указать должность и ФИО* администратором безопасности информации.

3. Утвердить:

Регламент использования сервисов электронной почты и информационно-телекоммуникационных сетей международного информационного обмена (Приложение №\_\_);

Перечень защищаемых информационных ресурсов (Приложение №\_\_);

Инструкцию должностного лица, ответственного за защиту информации (Приложение №\_\_);

Порядок допуска должностных лиц и обслуживающего персонала в помещения, в которых ведётся обработка защищаемых информационных ресурсов и обрабатывающим их техническим средствам, в рабочее и нерабочее время, а также в нештатных ситуациях (Приложение №\_\_);

Правила разграничения доступа к защищаемым информационным ресурсам, обрабатываемым с использованием средств вычислительной техники (Приложение №\_\_);

Порядок учета, хранения и уничтожения носителей защищаемых информационных ресурсов (Приложение №\_\_);

Инструкция по антивирусной защите информации (Приложение №\_\_);

Инструкция по организации парольной защиты (Приложение №\_\_);

3. Контроль за исполнением настоящего распоряжения *оставляю за собой/назначаю на заместителя руководителя ОРГАНИЗАЦИЯ.*

*Руководитель ОРГАНИЗАЦИЯ*

**Регламент использования сервисов электронной почты и информационно-телекоммуникационных сетей международного информационного обмена**

1. **Общие положения** 
   1. Регламент разработан на основании Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 № Пр-1895, Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», приказа Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» и других нормативных правовых документов в области информационной безопасности.
   2. Настоящий регламент определяет общий порядок использования сервисов электронной почты и информационно-телекоммуникационной сети международного информационного обмена Интернет.
   3. Основная цель регламента - предотвращение несанкционированного копирования, уничтожения, искажения и блокирования государственных информационных ресурсов, обрабатываемых с использованием средств вычислительной техники.
2. **Источники угроз информационной безопасности** 
   1. Подключение средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена представляет реальную угрозу регулярного несанкционированного контроля информационных процессов, несанкционированного доступа (НСД) и иным неправомерным действиям в отношении государственных информационных ресурсов и системам.
   2. Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть угрозы безопасности информации в результате таких действий как:

проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;

перенос в информационные системы (ИС) разрушающего программного обеспечения (внедрение программных закладок, вирусов);

выбор и использование законным пользователем системы неудачных паролей;

несанкционированная передача служебной информации ограниченного распространения, конфиденциальной информации и иной защищаемой информации пользователями в международные информационные сети (МИС) общего пользования и т.д.

* 1. При непосредственном подключении локальной вычислительной сети (ЛВС) к МИС общего пользования есть возможность:

получить информацию об адресной структуре сети;

установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);

получить информацию о пользователях сети;

попытаться получить доступ к защищаемым информационным ресурсам сети;

вызвать отказ в обслуживании легальных пользователей.

* 1. Кроме явных, непосредственно направленных на ЛВС, внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением вредоносного программного кода внутренними пользователя. К вредоносному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов и т.д.
  2. По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное подключение модемов (USB-модемов) к рабочим станциям пользователя, а также USB-накопителей информации, используемых для переноса информации из любых внешних информационных или автоматизированных систем. Причем подключение модемов не обязательно может использоваться для доступа в Интернет (возможны соединения к серверам других организаций, и к отдельным компьютерам, например домашним).

1. **Технические средства защиты информации** 
   1. К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет относятся системы разграничения прав доступа, межсетевые экраны, системы построения защищенных виртуальных сетей (Virtual Private Network – VPN), системы обнаружения атак, системы анализа защищенности, системы антивирусной защиты и т.д.
   2. Технические средства защиты отвечают требованиям безопасности информации и позволяют обеспечить эффективную защиту информации с высшей вероятностью только в том случае если администраторами и пользователями выполняются в комплексе организационные и технические меры по их применению.
   3. Системы разграничения доступа.

Система разграничения доступа ограничивает посторонним лицам доступ к ресурсам автоматизированной системы и позволяет разграничить права пользователей при работе на компьютере, при этом контролируются права локальных и удаленных пользователей.

* 1. Межсетевые экраны (МСЭ).

Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за потоками информации, поступающей в автоматизированную систему (АС) и(или) выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Межсетевые экраны позволяют осуществить: контроль доступа на межсетевом уровне, протоколирование информационных потоков, сокрытие топологии защищаемой сети, реагирование на несанкционированные действия.

Средствами МСЭ могут быть выявлены следующие виды атак: сканирование сетевых портов, атаки на отказ в обслуживании, изучение топологии внутренней сети, использование слабостей протоколов прикладного уровня, распространение вирусов и спама.

Основные показатели защищенности МСЭ: идентификация и аутентификация, регистрация событий и оповещение, контроль целостности, восстановление работоспособности.

* 1. Системы построения защищенных виртуальных сетей.

Системы построения защищенных виртуальных сетей позволяют организовать прозрачное для пользователей соединение локальных вычислительных сетей с помощью шифрования.

* 1. Системы обнаружения атак.

К системам обнаружения атак можно отнести: системы обнаружения атак на уровне сети, системы обнаружения атак на уровне хоста. Системы обнаружения атак используют:

- системы обнаружения аномального поведения пользователя (большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, использование периферийных устройств, которые обычно пользователем не используются и т.д.);

- системы обнаружения злоупотребления (обнаружение уже известной атаки по шаблону или «сигнатуре»).

* 1. Системы анализа защищенности.

Средства анализа защищенности предназначены для поиска в вычислительной технике и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак.

1. **Организация работы** 
   1. На автоматизированных рабочих местах должно быть установлено только программное обеспечение, необходимое для функционирования системы и выполнения администратором или пользователем своих функциональных (должностных) обязанностей.
   2. Владельцам открытых и общедоступных государственных информационных ресурсов необходимо осуществлять их включение в состав объектов сетей МИС только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.
   3. Пользователь АРМ обязан:

знать и строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

в пределах своей компетенции знать и строго выполнять правила работы со средствами защиты информации, используемых на персональных компьютерах;

хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты установленной на АС;

знать порядок входа в МИС общего пользования и регистрации в сети;

при пользовании электронной почтой не передавать сведения, содержащих конфиденциальную информацию и иную защищаемую информацию;

не распространять противозаконные материалы.

С целью предотвращения заполнения почты ненужной почтовой рекламной и другой информацией (спамом) запрещается размещать адрес своего электронного ящика на досках (доски объявлений) объявлений МИС.

* 1. Все АРМ оснащаются, в обязательном порядке, антивирусным программным обеспечением, обновление антивирусной базы которого производится регулярно. Антивирусное программное обеспечение настраивается на проверку всех файлов без исключения. При использовании съемных накопителей информации для передачи информации, каждый из них должен быть проверен на отсутствие вредоносного программного обеспечения. АС регулярно, не реже одного раза в неделю, проверяются на отсутствие вредоносного программного кода.
  2. При отправке электронных сообщений рекомендуется заполнять поле тема. Не рекомендуется открывать для чтения почтовые сообщения, адресат которых неизвестен или почтовое отправление носит подозрительный характер (реклама или запрос информации неизвестной фирмы, спам, и т.д.).
  3. Вредоносный программный код не может распространяться в составе самих сообщений электронной почты, но может содержаться в присоединенных к письму файлах, если это исполняемые файлы или файлы Word или Excel. Не рекомендуется загружать указанные типы файлов без предварительной антивирусной проверки.
  4. Если обнаружено, что почтовое отправление, пришедшее от адресата, заражено вредоносным кодом, необходимо:

срочно принять все меры по предотвращению дальнейшего распространения заражения путем прекращения приема передачи сообщений данной АС;

провести сканирование и лечение системы антивирусными средствами (при необходимости обновить базы данных антивирусного программного обеспечения);

сообщить адресату о наличии у него заражения, для последующего принятия адресатом срочных мер.

Запрещается хранение вредоносного кода, на каких-либо носителях информации.

При обнаружении вредоносного кода необходимо произвести его лечение антивирусными средствами. Удаление зараженных файлов средствами операционной системы может привести к безвозвратному разрушению информации.

1. **Работа в сети Интернет** 
   1. Пользователи могут осуществлять поиск и использовать ресурсы сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.
   2. При работе в сети Интернет, запрещено:

обмениваться конфиденциальной информацией и иной защищаемой информацией;

использование ресурсов сети Интернет для развлечения и получения информации, не относящейся к функциональным обязанностям пользователя;

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

открытие (запуск на выполнение) файлов, размещённых в сети Интернет;

загружать на компьютер материал, который является непристойным или нарушает законодательство Российской Федерации.

* 1. При необходимости переноса рабочих материалов, полученных из сети Интернет, на персональный компьютер пользователя, необходима их проверка антивирусными программными средствами.

1. **Порядок осуществления доступа и обмена данными с внешними по электронной почте** 
   1. При работе с электронной почтой пользователям запрещается:

обмен конфиденциальной информацией и иной защищаемой информацией;

предоставление доступа к электронной почте с использованием данных своей учетной записи другим лицам;

публикация своего служебного адреса электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей;

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

открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением.

* 1. Электронная почта предоставляется только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.
  2. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.
  3. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

1. **Ответственность** 
   1. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.
   2. Нарушение правил регламента может повлечь за собой принятие мер дисциплинарного и административного воздействия.

­**Перечень защищаемых информационных ресурсов в *ОРГАНИЗАЦИЯ***

1. Настоящий перечень разработан в целях исполнения законодательства Российской Федерации, регулирующего отношения, возникающие при осуществлении права на производство, поиск, получение, хранение, передачу, и распространение информации.
2. При разработке учитывались положения федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27.07.2006  № 152 «О персональных данных», Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», «Специальных требований и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.
3. К защищаемым информационным ресурсам относятся:

*сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.*

*Руководитель ОРГАНИЗАЦИЯ*

Инструкция должностного лица, ответственного за защиту информации в *ОРГАНИЗАЦИЯ*

1. **Общие положения**
   1. Настоящая инструкция определяет основные функции и права ответственного за защиту информации.
   2. Ответственный за защиту информации назначается руководителем *ОРГАНИЗАЦИЯ*.
   3. Ответственный за защиту информации проводит свою работу согласно нормативным правовым актам Российской Федерации, методическим и нормативным документам Российской Федерации, организационно-распорядительным документам по обеспечению безопасности информации, утверждённым в *ОРГАНИЗАЦИЯ*.
2. **Основные функции ответственного за защиту информации**
3. 1. Основными функциями ответственного за защиту информации являются:
4. проведение единой политики по обеспечению безопасности информации в *ОРГАНИЗАЦИЯ*;
5. осуществление контроля за соблюдением нормативных документов об обеспечении безопасности информации работниками *ОРГАНИЗАЦИЯ*;
6. организация и контроль мероприятий по техническому обеспечению безопасности информации при ее обработке на средствах вычислительной техники, в том числе мероприятий:

* по реализации разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам и информационным системам, содержащим защищаемую информацию;
* по разграничению доступа пользователей и обслуживающего персонала к защищаемой информации, программным средствам обработки (передачи) и защиты информации.

1. учет и хранение съемных носителей информации, содержащих защищаемую информацию, исключающих их хищение, подмену и несанкционированное уничтожение;
2. определению программного обеспечения, разрешенного к установке и (или) запуску, или исключению возможности установки и (или) запуска, запрещенного к использованию в программного обеспечения;
3. участие в разработке (доработке) организационно-распорядительных документов по обеспечению безопасности информации в *ОРГАНИЗАЦИЯ*;
4. информирование органа исполнительной власти Ленинградской области уполномоченного по защите информации о выявленных фактах нарушения установленного порядка и попытках несанкционированного доступа к защищаемым информационным ресурсам;
5. разработка предложений, участие в проводимых работах по совершенствованию системы защиты информации в *ОРГАНИЗАЦИЯ*;
6. присутствие при выполнении технического обслуживания элементов АРМ сторонними физическими лицами и организациями;
7. обращение в орган исполнительной власти Ленинградской области уполномоченный по защите информации, в случае возникновения внештатных ситуаций и аварийных ситуаций в АСЗИ, с целью ликвидации их последствий.
8. **Права ответственного за защиту информации**
   1. Ответственный за защиту информации имеет право:
9. запрашивать и получать в рамках своей компетенции необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности информации;
10. разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности информации в *ОРГАНИЗАЦИЯ*;
11. контролировать деятельность структурных подразделений организации в части выполнения ими требований по обеспечению безопасности информации;
12. вносить предложения руководителю *ОРГАНИЗАЦИЯ* о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) защищаемой информации;
13. запрещать устанавливать на рабочих станциях нештатное программное и аппаратное обеспечение;
14. инициировать расследование по фактам нарушения работниками *ОРГАНИЗАЦИЯ* законодательства Российской Федерации, в том числе требований, которые могут привести к снижению уровня защищенности информации.

**Порядок допуска должностных лиц и обслуживающего персонала в помещения *ОРГАНИЗАЦИЯ*, в которых ведётся обработка защищаемых информационных ресурсов и обрабатывающим их техническим средствам, в рабочее и нерабочее время, а также в нештатных ситуациях**

1. Настоящий порядок, устанавливает единые требования к допуску должностных лиц и обслуживающего персонала в служебные помещения, в которых ведётся обработка защищаемой информации (далее – служебные помещения) и обрабатывающим их техническим средствам.
2. Для служебных помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки и защиты информации, препятствующий возможности неконтролируемого проникновения или пребывания посторонних лиц, не имеющих право доступа в такие помещения.
3. При обработке в служебных помещениях, информации, содержащейся в государственных информационных системах, должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом должны предусматривать:

а) определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

б) санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

в) учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

1. В служебных помещениях, в которых размещаются информационные системы персональных данных и где размещены используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, необходимо обеспечение режима безопасности, который достигается путем:

а) оснащения таких помещений входными дверьми с замками, обеспечения постоянного закрытия дверей на замок и их открытия только для санкционированного прохода, а также опечатывания их по окончании рабочего дня или оборудование таких помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии;

б) утверждения перечня лиц, имеющих право доступа в такие помещения (Приложение № 1).

1. Служебные помещения располагаются в пределах контролируемой зоны, границами которой являются ограждающие конструкции зданий, в которых они размещены, с учётом территорий, контролируемых службами охраны.
2. Вскрытие и закрытие (опечатывание) служебных помещений, производится должностными лицами, имеющими право доступа в данные помещения.
3. Должностные лица, имеющие право доступа в служебные помещения не должны:

оставлять в свое отсутствие незапертым служебное помещение;

оставлять в служебном помещении посторонних лиц, не имеющих право доступа в такое помещение, без присмотра.

1. Обслуживание и сопровождение технических и программных средств, уборка, проведение других работ в служебных помещениях осуществляются в присутствии должностного лица, имеющего право доступа в данное помещение.
2. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка защищаемой информации, в нерабочее время, вскрытие служебного помещения осуществляется сотрудником службы безопасности, который ставит в известность ответственного по защите информации и должностных лиц, имеющих право допуска в данное помещение, в начале следующего рабочего дня.
3. Ответственность за соблюдение настоящего порядка возлагается на начальников отделов (структурных подразделений), в которых ведется обработка защищаемых информационных ресурсов.

*Руководитель ОРГАНИЗАЦИЯ*

Приложение № 1

Перечень лиц, имеющих право доступа в помещения, в которых размещаются информационные системы персональных данных и где размещены используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ

|  |  |
| --- | --- |
| Наименование должности | Номер помещения |
|  |  |
|  |  |

*Руководитель ОРГАНИЗАЦИЯ*

**Правила разграничения доступа к защищаемым информационным ресурсам, обрабатываемым с использованием средств вычислительной техники в *ОРГАНИЗАЦИЯ***

1. **Общие положения**
   1. Настоящие правила предназначены для установления правомерного порядка доступа должностных лиц к защищаемым информационным ресурсам, обрабатываемым в электронном виде с использованием средств вычислительной техники.
2. **Предоставление прав доступа к защищаемым информационным ресурсам**
   1. Предоставление прав доступа к информационным ресурсам реализуется в форме разрешительной системы доступа и основывается на функциональных обязанностях, выполняемых должностными лицами, связанных с обработкой защищаемых информационных ресурсах, с учетом требований, предъявляемых к безопасности информации.
   2. Реализация разрешительной системы доступа обеспечивается определением перечня должностных лиц, имеющих право доступа к защищаемым информационным ресурсам и предоставлением или ограничением такого доступа с помощью технических и программных средств защиты информации.
   3. Перечень должностных лиц, имеющих право доступа к защищаемым информационным ресурсам (Приложение № 1) утверждается *руководителем ОРГАНИЗАЦИЯ*.
   4. Предоставление или ограничение доступа к информационным ресурсам реализуется с помощью технических и программных средств защиты информации, прошедших установленным порядком процедуру оценки соответствия в форме обязательной сертификации по требованиям безопасности информации (далее – технические средства).
   5. С помощью технических средств осуществляется заведение, активация, блокирование или уничтожение соответствующих типов учетных записей (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей) и управление предоставления прав доступа.
   6. Управление правами доступа реализуются администратором безопасности информации на основании заявки должностного лица, в отношении которого принимаются меры по разграничению доступа к информационным ресурсам.
3. **Ответственность** 
   1. Администратор безопасности информации несёт ответственность за правильность настроек параметров технических средств разграничения доступа.
   2. Пользователи, допущенные к защищаемым информационным ресурсам, несут ответственность за нарушение требований безопасности информации, в соответствии с действующим законодательством.

Приложение № 1

Перечень должностных лиц, имеющих право доступа к защищаемым информационным ресурсам в *ОРГАНИЗАЦИЯ*

|  |  |
| --- | --- |
| Наименование должности | Перечень информационных ресурсов, к которым необходим доступ |
| Наименование подразделения | |
|  | *сведения конфиденциального характера;*  *информация, содержащаяся в государственных информационных системах* |
|  |  |
|  |  |
|  |  |

*Руководитель ОРГАНИЗАЦИЯ*

Приложение № \_\_

Порядок учета, хранения и уничтожения материальных носителей защищаемых информационных ресурсов в *ОРГАНИЗАЦИЯ*

1. **Общие положения**
   1. Настоящий порядок, определяет организационно-техническое обеспечение процессов обращения и порядок учёта, маркировки, хранения, передачи другим лицам, ремонта, технического обслуживания и уничтожения носителей защищаемых информационных ресурсов.
   2. Действие установленного порядка распространяется на всех должностных лиц.
   3. Ответственность за исполнение настоящего порядка возлагается на лицо, ответственное за защиту информации.
2. **Материальные носители информации**
   1. В настоящем документе рассматриваются следующие виды материальных носителей информации:

* машинные носители информации (МНИ);
* носители информации на бумажной основе.
  1. Машинные носители информации – изделия и устройства, предназначенные для записи и обработки информации входящие в состав средств вычислительной техники (СВТ), а также для хранения и перемещения записанной информации на внешние носители информации.

Виды МНИ:

* жесткие магнитные диски;
* гибкие магнитные диски;
* оптические и магнитооптические диски;
* устройства долговременной электронной памяти «Flash Memory»;

Типы МНИ:

а) съемные носители информации, устанавливаются и/или подключаются к СВТ на время сеанса работы пользователя, а по окончанию его отключаются и хранятся в определенном хранилище;

* несъемные носители информации в процессе работы пользователя не снимаются и не изымается из состава СВТ автоматизированной системы и находится там постоянно.
  1. Носители информации на бумажной основе – материальные носители графической и буквенно-цифровой информации, отраженной (зафиксированной) на бумаге.

1. **Порядок обращения с материальными носителями защищаемых информационных ресурсов**
   1. Все МНИ подлежат обязательному учету в «Журнале учета машинных носителей защищаемых информационных ресурсов» (Приложение № 1).
   2. Ответственность за ведение журнала возлагается на ответственного за защиту информации.
   3. Учет бумажных носителей информации осуществляется в соответствии с установленными правилами делопроизводства.
   4. Выдача МНИ фиксируется в документе «Журнал учета машинных носителей защищаемых информационных ресурсов» и подтверждается подписью пользователя.
   5. Все МНИ должны маркироваться и содержать учетный номер, дату ввода в эксплуатацию, наименование органа исполнительной власти Ленинградской области (владельца МНИ).

МНИ содержащие биометрические персональные данные должны позволять идентифицировать информационную систему персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись.

* 1. Съемные носители информации маркируются этикеткой, закрепленной на лицевой стороне носителя.
  2. Несъёмные носители информации учитываются отдельно и (или) в составе СВТ. При этом маркируется сам носитель или корпус СВТ, в состав которого входит носитель.
  3. СВТ в состав которого входит МНИ, вскрывается в присутствии ответственного за защиту информации и должностного лица эксплуатирующего данное СВТ.

1. **Правила хранение носителей защищаемых информационных ресурсов**
   1. При хранении МНИ должны соблюдаться условия, обеспечивающие сохранность информации, и исключающие к ним несанкционированный доступ, хищение, подмену и уничтожение.
   2. Хранение и использование МНИ должно осуществляться в условиях, соответствующих техническим условиям изготовителя и не более установленного срока эксплуатации.
   3. Необходимо обеспечивать раздельное хранение материальных носителей персональных данных, обработка которых осуществляется в различных целях, а также носителей персональных данных от носителей, содержащих иную защищаемую информацию.
   4. Для хранения носителей информации используются хранилища (сейфы, металлические шкафы, и т.п.), оборудованные внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

В случае если на съемном МНИ хранятся только данные в зашифрованном с использованием средств криптографической защиты информации (СКЗИ) виде, допускается хранение таких носителей в служебных помещениях вне сейфов (металлических шкафов).

* 1. МНИ с резервными копиями защищаемой информации не выдаются для работы обычным пользователям и служат только для восстановления в случае аварии или поломки основного МНИ. МНИ с резервными копиями рекомендуется хранить в отдельном хранилище.
  2. В случае если на основании договора, хранение носителей поручено другому лицу, существенным условием такого договора является обязанность обеспечения таким лицом безопасности переданной ему защищаемой информации

1. **Порядок уничтожения носителей защищаемых информационных ресурсов**
   1. МНИ подлежат уничтожению в следующих случаях:

* достижения целей обработки информации или в случае утраты необходимости в их достижении, для носителей, уничтожение информации на которых невозможно без уничтожения самого носителя;
* выхода из строя, повреждение МНИ, в результате которого невозможно осуществлять корректную обработку информации с использованием данного носителя;
* возникновения иных обстоятельств, в результате которых необходимо уничтожить носители, содержащие защищаемую информацию.
  1. Уничтожение осуществляется ответственным за защиту информации, с составлением акта об уничтожении МНИ, которые хранятся не менее трех лет.
  2. Вышедшие из строя МНИ ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения.
  3. Уничтожение МНИ должно обеспечивать полное физическое и невосстановимое уничтожение информации, содержащейся на таких носителях.

1. **Права и обязанности работников при обращении с носителями защищаемых информационных ресурсов**
   1. Запрещается выносить носители из служебных помещений (за пределы контролируемой зоны) для работы с ними на дому, в гостиницах, общественном транспорте и т.д.
   2. Права на перемещение МНИ за пределы контролируемой зоны предоставлено только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функции).
   3. Запрещается принимать и передавать МНИ без соответствующего разрешения и оформления в установленном порядке.
   4. Должностное лицо, осуществляющее работу с МНИ, обязано работать только с вверенными ему МНИ. Самовольная передача МНИ другим лицам запрещается.
   5. Запрещается хранить МНИ на рабочих столах, либо оставлять их без присмотра.
   6. Руководители подразделений, в которых осуществляется работа с МНИ, должны пресекать действия, которые могут привести к хищению или разрушению носителей.
   7. О фактах утраты носителей немедленно должен быть поставлен в известность ответственный за защиту информации.

Приложение № 1

**Журнал учета машинных носителей защищаемых информационных ресурсов**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Учетный номер** | **Регистрационный номер** | **Вид (съемный/несъемный)** | **Тип(оптический /магнитный /flash) и его емкость** | **Дата поступления** | **Расписка в получении (ФИО, подпись, дата)** | **Расписка в обратном приеме (ФИО, подпись, дата)** | **Место хранения  (№ помещения)** | **Дата и номер акта об уничтожении** | **Примечание** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
|  |  |

Инструкция по антивирусной защите информации

1. **Общие положения**
   1. Настоящая инструкция определяет порядок реализации антивирусной защиты информации.
   2. Инструкция предназначена для лиц, ответственных за защиту информации, пользователей и администраторов безопасности информации.
   3. Ответственность за выполнение мероприятий по антивирусной защите информации на эксплуатируемых средствах вычислительной техники и соблюдение требований настоящей инструкции возлагается на пользователей и администратора безопасности информации.
   4. Периодический контроль состояния антивирусной защиты информации и выполнения пользователями требований настоящей инструкции осуществляется пользователями и администратором безопасности информации.
   5. Периодический контроль соблюдения порядка, установленного настоящей инструкцией, антивирусной защиты информации пользователями осуществляется ответственным за защиту информации.
2. **Правила при работе на автоматизированном рабочем месте с антивирусными средствами защиты информации** 
   1. Запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на автоматизированных рабочих местах (АРМ).
   2. Пользователи АРМ при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносного программного кода.
   3. Установка и настройка параметров средств антивирусной защиты на средствах вычислительной техники обеспечивается администратором безопасности информации.
   4. Средство антивирусной защиты должно быть настроено таким образом, чтобы в автоматическом режиме производился периодический антивирусный контроль объектов информатизации (автоматизированных рабочих мест, серверов, других средств вычислительной техники), а также проверка в режиме реального времени объектов (файлов) запускаемых с внешних источников (съемных машинных носителей информации, сетевых подключений и других внешних источников) на наличие вредоносных компьютерных программ (вирусов).
   5. Обязательному входному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники: программные средства общего и специального назначения, любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по каналам передачи данных, а также информация на съемных машинных носителях информации (CD-ROM, Flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой (записью на съемный машинный носитель информации).
   6. При повреждении программных средств и информационных массивов программными вирусами должны выполняться мероприятия по восстановлению их работоспособности.
3. **Правила обновления баз данных вирусных описаний**
   1. Обновление баз данных вирусных описаний средств антивирусной защиты, используемых для защиты серверов и рабочих станций, осуществляется централизовано. Обновление проводится без участия пользователей посредством механизма централизованного управления и обновления баз данных вирусных описаний.
   2. Для осуществления процедуры копирования антивирусных обновлений с серверов обновлений, находящихся в сети Интернет, необходимо использовать отдельное выделенное рабочее место. После этого новые антивирусные базы могут быть скопированы в общедоступную папку.
   3. Для рабочих станций, являющихся автономными с точки зрения централизованного управления, обновление баз данных вирусных описаний осуществляется сотрудниками, за которыми закреплены функции по установке и настройке средств антивирусной защиты информации или государственным казенным учреждением «Оператор «электронного правительства». В качестве источника обновлений может выступать общая папка, содержащая необходимые файлы, на одном из АРМ, или же внешний носитель информации.
4. **Правила проведения антивирусной проверки**
   1. Установка (изменение) системного и прикладного программного обеспечения должна осуществляться в соответствии с программной и эксплуатационной документацией, поставляемой вместе с ним. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена полная антивирусная проверка АРМ.
   2. Если для рабочей станции отсутствует централизованное управление средствами антивирусной защиты, пользователь, за которым закреплено АРМ, не реже одного раза в неделю в обязательном порядке должен выполнять сканирование всех жестких дисков рабочей станции на отсутствие вирусов.
   3. 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.) пользователь самостоятельно или совместно с администратором безопасности информации, должен провести внеочередной антивирусный контроль АРМ.
   4. В случае обнаружения при проведении антивирусной проверки зараженных вирусами файлов пользователь обязан:

* приостановить работу;
* принять меры по локализации программного вируса (отключить рабочую станцию от локальной вычислительной сети);
* произвести лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь провести антивирусный контроль;
* в случае повторного обнаружения вируса после произведённой процедуры лечения пользователь должен немедленно поставить в известность администратора безопасности информации и прекратить какие-либо действия на АРМ.
  1. Администратор безопасности информации проводит расследование факта заражения компьютерным вирусом, и устраняет последствия вирусного заражения.

**Инструкция по организации парольной защиты**

1. **Общие положения**
   1. Настоящая инструкция по организации парольной защиты устанавливает требования к порядку выбора, хранения, использования, периодичности смены и другим вопросам, связанным с применением механизмов парольной аутентификации при обработке защищаемой информации с использованием средств вычислительной техники.
   2. Положения настоящей инструкции распространяются на пользователей и администраторов безопасности автоматизированных информационных систем в защищенном исполнении (АСЗИ).
   3. Пароль для доступа к информационным ресурсам предоставляются пользователям администратором безопасности информации, при регистрации их в качестве пользователей.
   4. Общий контроль выполнения требований настоящей инструкции осуществляется руководителями структурных подразделений, использующих АСЗИ и ответственным за защиту информации в ОРГАНИЗАЦИЯ.
2. **Права и обязанности**
   1. При получении пароля пользователь обязан произвести его смену. В дальнейшем пользователь должен осуществлять смену своих паролей самостоятельно в соответствии с требованиями настоящей инструкции. Напоминание об истечении срока действия пароля осуществляется техническими средствами защиты информации и контролируется ответственным за защиту информации.
   2. Пользователи должны регулярно производить смену своих паролей не реже, чем раз в 90 дней.
   3. Внеплановая смена пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на работу в другое структурное подразделение) производится на следующий день после даты прекращения полномочий пользователя.
   4. Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.
   5. С целью предотвращения несанкционированного доступа к АРМ пользователей, а также к информационным ресурсам АСЗИ, с использованием чужих учетных записей (имен пользователей), пользователи обязаны блокировать экраны своих компьютеров в случае оставления ими своего рабочего места.
   6. Все выбираемые пользователями пароли должны отвечать следующим требованиям:

содержать не менее 8 символов;

содержать символы, набранные в разных регистрах (a-z, A-Z);

помимо букв, содержать также цифры, знаки препинания и/или специальные символы (0-9,!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./);

не являться словом из словаря, сленга, диалекта, жаргона и т.п.;

не являться установленными «по умолчанию» производителями программного и аппаратного обеспечения;

символы не должны повторяться более двух символов подряд;

не являться датой рождения, местом рождения или другой похожей информацией личного характера.

* 1. Пользователи могут выбрать легко запоминающиеся пароли, которые в то же время являются трудно угадываемыми для других лиц, если будет выполнено хотя бы одно из следующих условий:

при наборе слова на клавиатуре использованы клавиши, смещенные относительно нужных на один ряд вверх, вниз, вправо или влево;

слово набрано со смещением на определенное количество букв вверх или вниз по алфавиту;

комбинация цифр и обычного слова;

намеренно неправильное написание слова (но не обычная в данном слове орфографическая ошибка).

* 1. Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.
  2. Пользователю запрещается:

сообщать свой пароль кому-либо, включая коллег, руководителей и специалистов управление автоматизации и информатизации, по телефону, по электронной почте или какими-либо иными средствами;

хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ. Например, ни в каких приложениях пользователи не должны выбирать такую опцию конфигурации, как автоматическое сохранение пароля;

записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица. Например, пользователь ни при каких обстоятельствах не должен оставлять записанный пароль в любом виде на рабочем месте (на мониторе, на и под клавиатурой, в ящике рабочего стола и т.д.);

произносить свой пароль вслух;

использовать общие пароли совместно с другими пользователями АСЗИ.

* 1. Если кто-либо требует раскрытия пароля, следует сослаться на настоящую инструкцию или предложить обратиться за разъяснениями к ответственному за защиту информации.
  2. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя.
  3. Администраторам безопасности информации для выполнения ими своих служебных обязанностей ни при каких обстоятельствах не требуется знание паролей пользователей. Для этого администраторы имеют все необходимые полномочия в АСЗИ. В случае необходимости администраторы могут произвести смену пароля пользователя, о чем должны сообщить пользователю незамедлительно.

1. **Ответственность**
   1. Ответственность за доведение положений настоящей инструкции до всех пользователей АСЗИ и иных лиц в части их касающейся, а также контроль соблюдения требований документа возлагается на руководителей структурных подразделений, использующих АСЗИ и ответственного за защиту информации.
   2. Ответственность за выполнение инструкции возлагается на всех пользователей и администраторов безопасности АСЗИ.