Приложение 1
к приказу «Об информационной безопасности в ФАУ ДПО ИПКЛХ»

от «13» июля 2017 г. № 49-4/02

Федеральное агентство лесного хозяйства
(Рослесхоз)
Федеральное автономное учреждение
дополнительного профессионального образования
«Институт повышения квалификации работников лесного хозяйства»
(ФАУ ДПО ИПКЛХ)

УТВЕРЖДЕНО
приказом ФАУ ДПО ИПКЛХ
от 13 июля 2017 года
№ 49-4/02

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ФЕДЕРАЛЬНОГО АВТОНОМНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ИНСТИТУТ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ РАБОТНИКОВ ЛЕСНОГО ХОЗЯЙСТВА» (ФАУ ДПО ИПКЛХ)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об информационной безопасности при работе на персональных компьютерах в локальной вычислительной сети (далее по тексту – Положение) Федерального автономного учреждения дополнительного профессионального образования «Институт повышения квалификации работников лесного хозяйства» (далее по тексту – Институт) является локальным нормативным актом, содержащим нормы регулирующим отношения по обеспечению

информационной безопасности и установлению правил поведения пользователей персональных компьютеров при работе с локальной вычислительной сетью Института.

1.2. Настоящее Положение устанавливает правила организации и осуществления работы по сопровождению баз данных и по обеспечению информационной безопасности при работе на персональных компьютерах (далее – ПК) в локальной вычислительной сети (далее – ЛВС) Института.

1.3. Целью настоящего Положения является определение основных требований, обязательных для исполнения при работе на ПК в ЛВС Института.

1.4. Настоящее Положение разработано на основании и во исполнение Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», других федеральных законов, иных нормативных правовых актов Российской Федерации.

1.5. Настоящее Положение утверждается и вводится в действие приказом ректора Института.

1.6. Положение распространяется на выполнение любых работ посредством ПК.

1.7. Работники Института и иные лица, не работающие в Институте (далее - Пользователи) допускаются к работе на ПК только после ознакомления с настоящим Положением и приложениями являющимися его неотъемлемой частью. Ответственность за ознакомление с настоящим Положением несет руководитель соответствующего внутреннего организационного структурного подразделения, в котором, либо в компетенцию которого входит организация и осуществление работы на ПК.

1.8. Контроль за исполнением требований к информационной безопасности информационных систем Института возложено:

- по Институту в целом – на проректора;
- по работе на персональных компьютерах Института, установленному программному обеспечению – на ответственного за информационную безопасность;
- по работе с Интернетом, электронной почтой - на ответственного за информационную безопасность.

1.9. Ответственное должностное лицо за информационную безопасность при работе в локальной вычислительной сети Института, установку и обновление сетевого антивирусного программного обеспечения, своевременную установку заплат программных систем, а также за реализацию и исполнение настоящего Положения назначается приказом ректора Института.

2. ТРЕБОВАНИЯ К ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРАМ ИНСТИТУТА

2.1. Требования к ПК Института:

2.1.1. Все ПК должны быть подключены к локальной сети Института.

2.1.2. Опечатаны системные блоки.

2.1.3. Установлены на каждом используемом ПК антивирусное программное обеспечение.

2.1.4. Наличие паспорта на каждый используемый ПК, подписанный ответственным за информационную безопасность в Институте, с перечисленными в

нем техническими характеристиками, установленным системным программным обеспечением.

2.1.5. Наличие списка (реестра) пользователей ПК, допущенных к работе с указанием ответственного за эксплуатацию данного ПК.

2.1.6. Установлено антивирусное программное обеспечение на все используемые в Институте ПК.

2.1.7. Систематическое обновление антивирусных баз.

2.1.8. Вход в BIOS должен быть закрыт паролем, отключена загрузка ПК с внешних носителей (FDD, CD, LAN, …).

2.1.9. Систематически менять пароли пользователей на доступ к ПК не реже 1 раза в 3 месяца, для администраторов не реже 1 раза в месяц. Ведение реестра паролей установленных на ПК пользователей, который должен находиться в закрытом доступе.

2.1.10. Установлено для ПК с процессором 3-го поколения и выше файловая система основного раздела - NTFS.

2.1.11. Папка для обмена информацией по ЛВС должна быть доступна на запись для файловых систем FAT, для систем NTFS - только на «Запись» и «Чтение содержимого папки». При наличие на ПК диска с файловой системой NTFS папка для обмена должна располагаться только на этом диске.

2.1.12. Осуществлять запись файлов содержащихся на ПК пользователей, а также файлы и баз данных содержащихся на жестком диске сервера Института не реже 1 раза в 2 месяца в целях сохранности информации при сбоях системы.

2.2. Решение об изменении предъявляемых требований к отдельным ПК принимается ответственным за информационную безопасность по мотивированному ходатайству руководителя структурного подразделения. Перечень данных ПК хранится у ответственного за информационную безопасность.

2.3. Копирование информации на ПК с отключенными устройствами для работы со сменными носителями информации осуществляет через ответственного за информационную безопасность по письменному ходатайству руководителя соответствующего структурного подразделения Института.

3. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ПРАВ ДОСТУПА К ПК, ПРОГРАММАМ И РЕСУРСАМ ЛВС ИНСТИТУТА

3.1. Предоставление работникам Института прав доступа к необходимым для работы программам локальной сети Института осуществляется по заявке руководителя внутреннего организационного структурного подразделения. При изменении должностных обязанностей сотрудника руководитель структурного подразделения направляет на ответственного за информационную безопасность служебную записку на аннулирование прав доступа.

3.2. Предоставление лицам, не работающим в Институте, прав доступа к необходимым для работы программам локальной сети Института, осуществляется по служебной записке ответственному за информационную безопасность от руководителя соответствующего внутреннего организационного структурного подразделения.

3.4. Руководитель соответствующего внутреннего организационного структурного подразделения своим распоряжением определяет перечень сотрудников соответствующего подразделения, имеющих доступ к каждому конкретному ПК.

3.5. Постоянный доступ к сети Интернет и служебным почтовым ящикам предоставлять по письменному разрешению (приказа) ректора Института.

4. ЗАПРЕТЫ ПРИ РАБОТЕ С ЛВС ИНСТИТУТА

4.1. Пользователям ПК Института запрещается:

4.1.1. Использовать компоненты программного и аппаратного обеспечения в неслужебных целях.

4.1.2. Посещать в Интернет сайты, содержащие информацию, не входящую в круг служебных обязанностей работника.

4.1.3. Изменять параметры сетевой идентификации компьютера (имя, IP адрес).

4.1.4. Предоставлять права удаленного доступа к системным ресурсам своего ПК (корневой раздел жесткого диска, на котором установлена операционная система, каталоги, в которых установлена операционная система).

4.1.5. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые системные программные и аппаратные средства, не предусмотренные паспортом ПК.

4.1.6. Отключать свой ПК от локальной сети Института.

4.1.7. Снимать пломбу с компьютера.

4.1.8. Предоставлять закреплённый за ними ПК в пользование другим лицам или сотрудникам, не имеющим права доступа за исключением ответственного за информационную безопасность.

4.1.9. Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.).

4.1.10. Оставлять включенный без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры).

4.1.11. Оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения).

4.1.12. Использовать и хранить на рабочих местах съемные носители информации (Flash-карты, и т.п., в том числе цифровые фотокамеры) без специального разрешения.

4.1.13. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению конфликтной ситуации. Об обнаружении такого рода ошибок ставить в известность техника-программиста II категории и руководителя своего структурного подразделения.

4.1.14. Предпринимать попытки взлома компьютерной защиты ПК других пользователей, локальной сети Института, ресурсов сторонних организаций.

4.1.15. Предпринимать действия, направленные на несанкционированное получение прав доступа к программам, базам данных и иной информации, хранящейся в локальной сете Института, на ПК других пользователей.

4.1.16. Сообщать кому бы то ни было, кроме непосредственного руководителя (записывать в доступном месте), свой пароль (пароли).

4.1.17. Посылать в электронном виде информацию, содержащую сведения ограниченного распространения без применения программного обеспечения для ее защиты.

4.1.18. Использовать файлы, полученные по почте, через Интернет или со сменных носителей без предварительной проверки на наличие вирусов;

4.1.19. Получать и использовать удалённый доступ на управление ПК других пользователей и серверов.

5. ДЕЙСТВИЯ ПРИ ВОЗНИКНОВЕНИИ НЕИСПРАВНОСТЕЙ

5.1. В случае неправильной работы программного обеспечения, обнаружении вирусов, технической неисправности ПК пользователь обязан незамедлительно ставить в известность техника-программиста II категории.

5.2. В случае проблем при работе с информационно-телекоммуникационной сетью «Интернет» и электронной почтой пользователь обязан незамедлительно обращаться техника-программиста II категории.

6. РАЗГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Ответственность за безопасность загруженной информации через информационно-телекоммуникационную сеть «Интернет» и электронную почту, возлагается на пользователя, осуществившего приём этой информации. Если пользователь не выявлен, то ответственность несёт лицо, закреплённое за ПК.

6.2. Ответственность за информационную безопасность при работе в ЛВС Института, установку и обновление сетевого антивирусного программного обеспечения, своевременную установку заплат программных систем возлагается на должностное лицо ответственное за информационную безопасность в Институте.

7. ОТВЕТСТВЕННОСТЬ

7.1. За неисполнение требований по информационной безопасности руководители внутренних организационных структурных подразделений Института, и пользователи несут административную и дисциплинарную ответственность.

7.2. Ответственность за сохранность пломб, установленных на ПК несет пользователь ПК. В случае нарушения целостности пломб, ответственный за информационную безопасность проводится служебное расследование, с целью выявления нарушения и составления акта.

7.3. За неисполнение или ненадлежащее исполнение норм, предусмотренных настоящим Положением работники Института и иные лица несут дисциплинарную,

материальную, гражданско-правовую, административную и уголовную ответственность в зависимости от тяжести проступка.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение вступает в силу с момента утверждения.

8.2. Настоящее Положение утверждается и вводится в действие приказом ректора Института.

8.3. Изменения и дополнения к настоящему Положению утверждаются в форме проекта изменений к настоящему Положению и вводятся в действие приказом ректора Института.

8.4. Неотъемлемой частью настоящего Положения являются следующие приложения:

8.4.1. Инструкция пользователя компьютерной локальной вычислительной сети ФАУ ДПО ИПКЛХ (приложение 1).

8.4.2. Инструкции по организации антивирусной защиты в ФАУ ДПО ИПКЛХ (приложение 2).

8.4.3. Инструкция по проверке внешнего накопителя на наличие вирусов (приложение 3).

Приложение 1
к Положению об информационной безопасности
при работе на персональных компьютерах в локальной
вычислительной сети ФАУ ДПО ИПКЛХ
от «13» июня 2017 г.

Федеральное агентство лесного хозяйства
(Рослесхоз)
Федеральное автономное учреждение
дополнительного профессионального образования
«Институт повышения квалификации работников лесного хозяйства»
(ФАУ ДПО ИПКЛХ)

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРНОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ФАУ ДПО ИПКЛХ

1. Общие положения

1.1. Настоящая Инструкция является неотъемлемой частью Положение об информационной безопасности при работе на персональных компьютерах в локальной вычислительной сети Федерального автономного учреждения дополнительного профессионального образования «Институт повышения квалификации работников лесного хозяйства» (далее – Институт), которая определяет права и обязанности пользователей компьютерного оборудования в Институте.

1.2. Институт намерено придерживаться правил, изложенных ниже, и оставляет за собой право проверять их выполнение без предварительного уведомления пользователя.

1.3. Компьютерной локальной вычислительной сетью (далее - ЛВС) Института называется совокупность компьютеров, кабелей, сетевых адаптеров, работающих под управлением сетевой операционной системы и разрешенного прикладного программного обеспечения (далее - ПО) и оборудования, явно неуказанного в данной инструкции, но позволяющего использовать ресурсы ЛВС Института.

1.4. Локальная вычислительная сеть (ЛВС) предназначена для:

1.4.1. Предоставления разделенного доступа к файлам. ЛВС позволяет одновременно нескольким пользователям работать с одним и тем же файлом, хранящимся на центральном файл-сервере и производить с ним различные действия.

1.4.2. Передачи файлов. ЛВС позволяет быстро копировать файлы любого размера с одной рабочей станции на другую без использования переносных носителей информации.

1.4.3. Доступа к информации и файлам. ЛВС позволяет запускать прикладные программы на сервере с любой из рабочих станций, работать с базами данных и файлами, расположенными на сервере.

1.4.4. Предоставления разделенного доступа к принтерам. ЛВС позволяет нескольким пользователям на различных рабочих станциях использовать совместно один или несколько принтеров.

1.4.5. Удаленного доступа к оборудованию.

1.5. Персональные компьютеры (далее - ПК), серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование ЛВС, коммуникационные средства являются собственностью Института и предоставляются работникам для осуществления ими их должностных обязанностей.

1.6. ПК, серверы, ПО, оборудование корпоративной ЛВС Института, коммуникационное оборудование и пользователи, образуют систему корпоративной локальной сети Института.

1.7. Целью настоящей инструкции является:

1.7.1. Регулирование работы пользователей с компьютерным оборудованием, ЛВС и ПО.

1.7.2. Распределение сетевых ресурсов коллективного пользования.

1.7.3. Определение мер по поддержанию необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к ней, обеспечение использования только лицензионного ПО.

1.7.4. Уменьшение рисков умышленного или неумышленного неправильного использования сетевых ресурсов, ПО.

1.7.5. Упорядочивание использования компьютерного оборудования корпоративной ЛВС Института с целью повышения эффективности выполнения производственных планов и осуществления другой деятельности предусмотренной производственной необходимостью.

1.7.6. Предотвращение ненадлежащего использования компьютерного оборудования, ЛВС и ПО.

1.8. Действие настоящих правил распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, коммуникационное оборудование), подключенного к ЛВС учреждения, а также на пользователей, осуществляющих удаленный доступ к оборудованию из ЛВС учреждения и удаленный доступ к ЛВС учреждения.

2. Правила работы с локальной вычислительной сетью Института

2.1. К работе с ЛВС учреждения допускаются лица, назначенные начальниками соответствующих отделов и подразделений, прошедшие инструктаж, регистрацию и получившие соответствующие уникальные средства аутентификации в ЛВС учреждения - это учётная запись (логин) пользователя и пароль, в отделе системного администрирования и закрепленные за определенным компьютером.

2.2. Работа с ЛВС Института каждому работнику разрешена только на определенных компьютерах, в определенное время (в пределах установленного рабочего графика), только со своей, полученной у техника-программиста учетной

записью пользователя и паролем, и только с разрешенными программами и сетевыми ресурсами. В случае необходимости выполнения работ вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение техника-программиста.

2.3. Пользователь самостоятельно создает пароль для входа в ЛВС Института. Пароль должен содержать не менее 5 (пяти) символов. Пароль не должен привязываться к дням рождения пользователя или его номера телефона и прочей информации, которая может быть легко подобрана путем сопоставления с данными пользователя. Изменение пароля на новый должно проводиться пользователем не реже 1-го раза в 3 месяца, а для техника-программиста не реже 1-го раза в месяц.

2.4. Пользователь, подключенного к ЛВС компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

2.5. Для работы на компьютере других лиц, кроме закрепленного за ним пользователя и его начальника отдела (подразделения), необходимо получить разрешение у техника-программиста. Никто не может давать разрешение даже на временную работу на компьютере, без получения разрешения у техника-программиста. После получения соответствующего разрешения, пользователь обязан зарегистрироваться на компьютере, под своей, полученной у техника-программиста, учетной записью (логином).

2.6. В случае выявления нарушений инструкции пользования ЛВС Института, техник-программист имеет право отстранить виновного от пользования компьютером или принять иные меры, необходимые для предотвращения выявленного нарушения, и сообщить о таком факте ректору.

2.7. Техник-программист имеет право отключить компьютер пользователя от ЛВС в случае, если с данного компьютера производились попытки несанкционированного доступа к информации других компьютеров, и при других серьезных нарушений настоящей инструкции. О данном факте техник-программист обязан незамедлительно сообщить ректору.

2.8. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им или каком-либо другом компьютере, о фактах использования неразрешенного или не лицензионного ПО, пользователь должен немедленно сообщить об этом технику-программисту. При этом, техник-программист обязан проанализировать поступившую информацию и безотлагательно уведомить ректора об указанных фактах.

2.9. Все пользователи ЛВС Института при подключении, получают ограниченный уровень доступа к ресурсам своих компьютеров (уровень пользователя) и обязаны работать только с разрешенным уровнем доступа. Для получения административного уровня доступа к ЛВС и ресурсам компьютера, необходимо письменно указать необходимость работы на компьютере и ЛВС Института с повышенным уровнем доступа и получить письменное разрешение у руководства Института (административный доступ к ресурсам необходим для корректной работы некоторого программного обеспечения — для этого техник-

программист может произвести дополнительные настройки данного ПО позволяющие работать ему с административным уровнем, при этом не предоставляя повышенных привилегий пользователю).

2.10.Техник-программист, с целью повышения уровня безопасности работы ЛВС Института, может без уведомления пользователей проводить соответствующие работы (инсталляция нового программного обеспечения по сети на компьютеры пользователей, сканирование на вирусы и др.)

3. Права и обязанности пользователей локальной вычислительной сетью Института

3.1. Пользователь ЛВС обязан:

3.1.1. Ознакомиться с настоящей инструкцией и правилами работы в ЛВС до начала работы на компьютерном оборудовании.

3.1.2. Соблюдать правила работы в корпоративной ЛВС, оговоренные настоящей Инструкцией.

3.1.3. Пользоваться только разрешенным ПО (необходимый перечень которого устанавливается приказом ректора) и не допускать использования ПО с нарушением лицензионных условий.

3.1.4. Пройти инструктаж и получить личные уникальные средства аутентификации в ЛВС Института (имя пользователя, пароль) для работы с оборудованием с ограниченным доступом.

3.1.5. Использовать индивидуальное имя пользователя для своей идентификации в сети. Индивидуальное имя пользователя назначается техником-программистом.

3.1.6. При доступе к внешним ресурсам ЛВС, соблюдать правила, установленные техником-программистом, для используемых и разрешенных ресурсов.

3.1.7. Пользоваться только своим именем пользователя и паролем для входа в локальную сеть. Передача таких данных кому-либо запрещена.

3.1.8. Использовать компьютерное оборудование исключительно для деятельности, предусмотренной производственной необходимостью и должностными инструкциями.

3.1.9. Бережно относиться к оборудованию, соблюдать правила его эксплуатации.

3.1.10. Рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров общего пользования, пропускной способностью локальной сети) и расходными материалами.

3.1.11. Выполнять требования техника-программиста, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования.

3.1.12. Выполнять обязательные рекомендации и предписания техника-программиста, направленные на обеспечение безопасности ЛВС.

3.1.13. Предоставлять доступ к сетевому оборудованию и компьютеру технику-программисту для проверки исправности и соответствия установленным правилам работы.

3.1.14. Немедленно сообщать в технику-программисту об обнаруженных проблемах в использовании предоставленных ресурсов (несанкционированный доступ к оборудованию, информации, ее искажение или уничтожение), а также о фактах нарушения настоящей инструкции кем- либо. Техник-программист, при необходимости, с привлечением других специалистов, должен провести расследование указанных фактов и принять соответствующие меры.

3.1.15. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы ЛВС.

3.1.16. Немедленно отключить от ЛВС компьютер, при появлении сообщений антивирусного ПО о потенциальной опасности заражения, сообщить об этом технику-программисту и далее действовать по его указаниям.

3.1.17. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь обязан сообщить об этом технику-программисту.

3.2. Пользователи ЛВС имеют право:

3.2.1. Подать заявку технику-программисту на получение прав доступа к оборудованию общего пользования.

3.2.2. Подавать заявки на закупку нового и модернизацию компьютерного оборудования персонального пользования.

3.2.3. Получать консультацию техника-программиста по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

3.2.4. В случае несогласия, обжаловать руководителю подразделения действия техника-программиста.

3.2.5. Использовать в работе предоставленные им и разрешенные сетевые ресурсы, в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с техником-программистом. Техник-программист вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

3.2.6. Обращаться к технику-программисту по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка общего доступа к папкам компьютера), должны санкционироваться техником-программистом.

4. Ограничения (запреты) при работе с локальной вычислительной сетью Института

4.1. Пользователям ЛВС запрещается:

4.2. Допускать посторонних лиц к работе на закрепленном компьютере (кроме случаев связанных с выполнением работ техником-программистом, в рамках своих служебных и должностных обязанностей, или по указанию руководителя отдела).

4.3. Использовать оборудование, сетевые программы для деятельности, не обусловленной производственной необходимостью и должностной инструкцией.

4.4. Создавать помехи работе других пользователей, помехи работе компьютеров и сети.

4.5. Самостоятельно устанавливать или удалять любое ПО на компьютерах, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов. Установку, удаление, модернизацию, настройку операционной системы, ПО и иные подобные действия на компьютере пользователя, - выполняют ТОЛЬКО техник-программист.

4.6. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.7. Вскрывать компьютеры, сетевое и периферийное оборудование, разбирать, изменять настройку оборудования общего пользования, подключать к компьютеру дополнительное оборудование без ведома техника-программиста, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет, дисков, FLASH- накопителей и др. Перемещение компьютерного оборудования допускается в исключительных случаях, а именно: пожарной опасности, других угроз жизни и здоровью людей или угроз повреждения имущества.

4.8. Самовольно подключать компьютер к ЛВС Института, а также изменять IP и MAC-адрес компьютера, выданный техником-программистом, устанавливать дополнительные сетевые протоколы, изменять конфигурацию настроек сетевых протоколов без предварительного уведомления техника-программиста. Передача данных в сеть с использованием других IP и MAC адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.

4.9. Работать с каналоемкими ресурсами (трансляция видео, трансляция аудио, чаты и др.) без согласования с руководством Института и техником-программистом.

4.10.Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, которая охраняется законодательством об интеллектуальной собственности, либо задевающую честь и достоинство граждан, а также рассылать обманные, угрожающие и др. сообщения.

4.11.Предпринимать попытки обхода учетной системы безопасности, системы статистики, ее повреждения или дезинформации.

4.12.Использовать иные формы доступа к сети, за исключением разрешенных техником-программистом, пытаться обходить установленный межсетевой экран.

4.13.Осуществлять попытки несанкционированного доступа к ресурсам ЛВС, проводить или участвовать в сетевых атаках и сетевом взломе. Производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов ЛВС и передаваемой по сети информации, равно как и любых других компьютеров, в случае доступа к глобальной сети Интернет.

4.14.Использовать ЛВС для распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4.15.Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь не имеет права пользоваться чужими именами и паролями (случайно ставшими ему известными) для входа в сеть, читать чужую электронную почту, причинять вред данным, принадлежащих другим пользователям.

4.16.Закрывать доступ к информации паролями без согласования с начальниками отделов и техником-программистом.

4.17.Передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль) к компьютеру, а также предоставлять доступ к каналам сети пользователям других сетей (например, посредством proxy-server, socks-proxy, open relay и т.п.).

4.18.Использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы ими инфицированные, использовать, распространять и хранить программы сетевого управления и мониторинга, осуществляющих сканирование сети (различные «трассеры», «сниферы», сканеры портов и т.п.), без письменного предупреждения и разрешения техника-программиста, с объяснением служебной необходимости подобных действий.

4.19.Предоставлять доступ к компьютерному оборудованию незарегистрированным пользователям без согласования с техником-программистом.

4.20.Использовать в работе съемные носители информации без разрешения техника-программиста. Съемные носители информации, перед началом работы с ними, обязательно должны пройти проверку антивирусной программой.

4.21.Переносить информацию, связанную с деятельностью Института, с компьютера на компьютер (не распространяется, если перенос осуществляется внутри отдела).

4.22.Хранить информацию, связанную с деятельностью Института, в папках с общим доступом.

4.23.Хранить на публичных сетевых дисках и серверах файлы, не относящихся к выполнению служебных обязанностей сотрудника (музыка, фотографии, игры, видео, виртуальные CD и т.п.).

5. Работа с электронной почтой

5.1. Электронная почта предоставляется работникам Института только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

5.2. Все электронные письма, создаваемые и хранимые на компьютерах учреждения, являются собственностью Института и не считаются персональными.

5.3. Институт оставляет за собой право получить доступ к личной электронной почте работников, если на, то будут веские причины. Содержимое электронного письма не может быть раскрыто третьим лицам, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

5.4. В случае использования цифровых подписей в Институте почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось цифровой подписью отправителя.

5.5. В случае если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью Института, или другая важная информация, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в Институте программ и алгоритмов.

5.6. Вся информация, классифицированная как критическая, конфиденциальная или относится к коммерческой (служебной) тайне, при передаче ее через открытые сети, такие как Интернет, обязательно должна быть предварительно зашифрована.

5.7. Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности Института.

5.8. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

5.9. В качестве клиентов электронной почты могут использоваться только лицензионные программные продукты или утвержденные техником-программистом почтовые программы.

5.10.Категорически запрещено открывать или запускать приложения, полученные по электронной почте из неизвестного источника, с подозрительным названием и (или) не затребованные пользователем.

5.11.Запрещено осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается, как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5.12.Запрещено использовать несуществующие обратные адреса при отправке электронных писем.

5.13.Отправлять по электронной почте, большие файлы (особенно музыку, видео и фото личного характера), за исключением случаев, связанных со служебной необходимостью.

6. Работа с веб-ресурсами

6.1. Пользователям ЛВС предоставлено право использовать только разрешенные программы для поиска информации в сети Интернет и только для выполнения своих должностных обязанностей.

6.2. Использование ресурсов сети Интернет не должно создавать потенциальную угрозу Институту.

6.3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему соответствующих санкций.

6.4. Сотрудникам Института, пользующимся Интернетом, запрещено передавать (сохранять) материал, который является непристойным, содержит порнографическую информацию, нарушает законодательство РФ в части

использования объектов интеллектуальной собственности, а также не относящимся к деятельности Института.

6.5. Все программы, используемые для доступа к сети Интернет, не должны нарушать лицензионные условия их использования, утверждаются техником-программистом и в них должны быть настроены необходимые уровни безопасности.

6.6. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы/шпионское ПО с помощью утвержденных антивирусных программ.

6.7. При работе с веб-ресурсами запрещено:

6.7.1. Получать и передавать через ЛВС информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;

6.7.2. Получать доступ к информационным ресурсам ЛВС или сети Интернет, не являющихся публичными, без разрешения их собственника;

6.7.3. Играть в различные онлайн игры (онлайн казино и тому подобные);

6.7.4. Использовать различные сайты и программы для анонимного доступа в сеть Интернет;

6.7.5. Использовать программы для зарабатывания денег в сети интернет, таких как Spedia, Web Money и им подобных;

6.7.6. Скачивание музыкальных и видео файлов, а также файлов, не имеющих отношения к текущим служебным обязанностям работника, без согласования с руководством и техником-программистом.

7. Ответственность

7.1. Пользователь компьютера отвечает за всю информацию, хранящуюся на нем, технически исправное состояние вверенной ему техники.

7.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ЛВС и за ее пределами.

7.3. В зависимости от последствий невыполнения предписаний, предусмотренных в настоящей Инструкции, а также других обязательных условий работы с компьютерным оборудованием и ЛВС, пользователь может быть привлечен к дисциплинарной ответственности в соответствии трудовым законодательством и иными локальными нормативными актами Института по решению ректора на основании докладной записки техника-программиста с учетом мнения уполномоченного работниками представителя трудового коллектива.

7.4. Нарушение данной Инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или ЛВС компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством РФ, а также возмещение пользователем действительного ущерба, причиненного такими действиями.

7.5. Вся полнота ответственности за установку, использование и хранение на вверенном компьютерном оборудовании, ПК не утвержденного или не

лицензионного ПО, несанкционированное распространение информации, являющейся интеллектуальной собственностью, возлагается на пользователя.

Приложение 2
к Положению об информационной безопасности
при работе на персональных компьютерах в локальной
вычислительной сети ФАУ ДПО ИПКЛХ
от «13» июля 2017 г.

Федеральное агентство лесного хозяйства
(Рослесхоз)
Федеральное автономное учреждение
дополнительного профессионального образования
«Институт повышения квалификации работников лесного хозяйства»
(ФАУ ДПО ИПКЛХ)

ИНСТРУКЦИИ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ФАУ ДПО ИПКЛХ

1. Общие положения

1.1. Настоящая Инструкция является неотъемлемой частью Положение об информационной безопасности при работе на персональных компьютерах в локальной вычислительной сети Федерального автономного учреждения дополнительного профессионального образования «Институт повышения квалификации работников лесного хозяйства» (далее – Институт), которая определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) Института от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. К использованию в Институте допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка средств антивирусного контроля на серверах и рабочих станциях ИСПДн осуществляется администратором безопасности.

1.4. Настройка параметров средств антивирусного контроля осуществляется администратором безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD – ROM, Flash, SD и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

3. Действия при обнаружении вирусов

3.1. 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.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

3.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

3.2.1. приостановить работу;

3.2.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и ответственного за обеспечение информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;

3.2.3. администратор безопасности совместно с владельцем зараженных вирусом файлов должен провести анализ необходимости дальнейшего их использования;

3.2.4. провести лечение или уничтожение зараженных файлов;

3.2.5. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку или разработчику используемого антивирусного программного обеспечения;

3.2.6. по факту обнаружения зараженных вирусом файлов составить служебную записку и передать ее ответственному за информационную безопасность сотруднику, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3.3. Пользователям запрещается:

3.3.1. Отключать средства антивирусной защиты информации во время работы.

3.3.2. Открывать сомнительные эл. письма (необходимо удаление), ссылки, сайты, источники переноса информации.

4. Ответственность

4.1. Ответственность за организацию антивирусного контроля в внутренних организационных структурных подразделений Института, эксплуатирующем компьютерную технику, в соответствии с требованиями настоящей Инструкции возлагается на соответствующего руководителя структурного подразделения.

4.2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями компьютерной техники.

4.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками (пользователями ПК) внутренних организационных структурных подразделений Института осуществляется проректором и ответственным за информационную безопасность.

Приложение 3
к Положению об информационной безопасности
при работе на персональных компьютерах в локальной
вычислительной сети ФАУ ДПО ИПКЛХ
от «13» июня 2017 г.

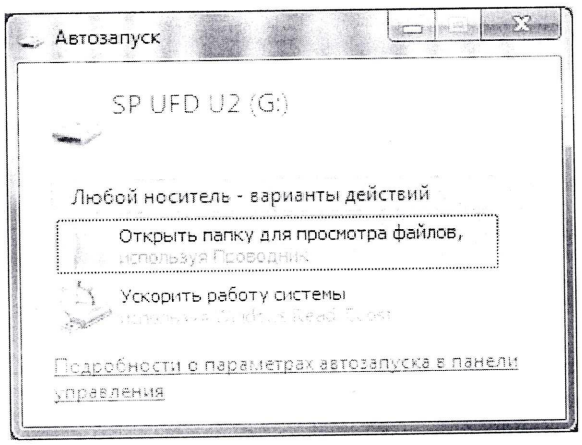
Федеральное агентство лесного хозяйства
(Рослесхоз)
Федеральное автономное учреждение
дополнительного профессионального образования
«Институт повышения квалификации работников лесного хозяйства»
(ФАУ ДПО ИПКЛХ)

ИНСТРУКЦИЯ ПО ПРОВЕРКИ ВНЕШНЕГО НАКОПИТЕЛЯ НА НАЛИЧИЕ ВИРУСОВ

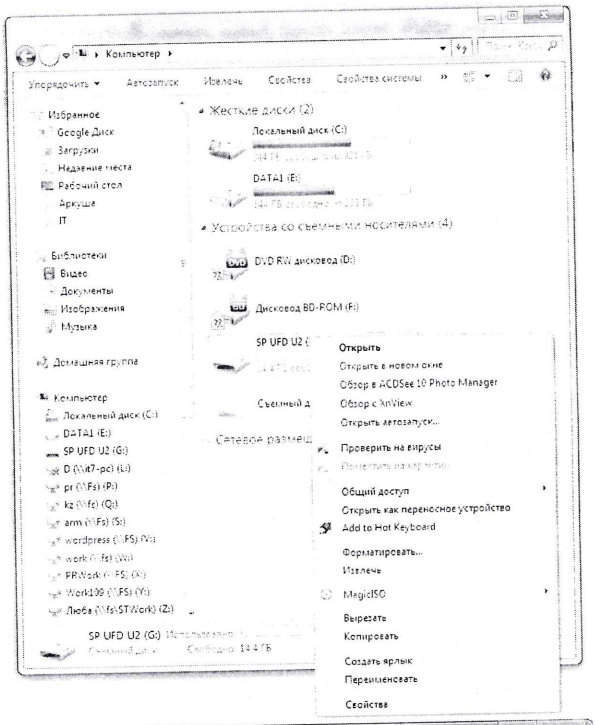
Настоящая Инструкция является неотъемлемой частью Положение об информационной безопасности при работе на персональных компьютерах в локальной вычислительной сети Федерального автономного учреждения дополнительного профессионального образования «Институт повышения квалификации работников лесного хозяйства».

Перед началом работы с внешним накопителем (USB Flash, SD, CD, DVD и т.д.) необходимо проверить его на наличие вирусов.

1. При подключении внешнего накопителя необходимо свернуть или закрыть окно автозапуска.



2. В окне мой компьютер открыть контекстное меню внешнего накопителя (правой кнопкой мыши по значку накопителя) и выбрать пункт «Проверить на вирусы».



3. Если в открывшимся окне по окончание проверки на вирусы сообщение «угрозы не обнаружены» его можно закрыть и начать работу с внешним накопителем. В противном случае, при обнаружении угроз, следует остановить работу с компьютером и обратиться к специалисту.