Гриф по заполнению

Экз. един.

Утверждаю
Директор ТОГАПОУ
«Аграрно-промышленный колледж»
_____И.Н.Михайлюк
24.11.2016

ИНСТРКУЦИЯ

по обеспечению безопасности информации в ТОГАПОУ «Аграрно-промышленный колледж» при взаимодействии абонентов с информационными сетями общего пользования и (или) сетями международного информационного обмена

1. Общие положения

1.1. Инструкция по обеспечению безопасности информации в ТОГАПОУ «Аграрно-промышленный колледж» при взаимодействии абонентов с информационными сетями общего пользования и (или) международного информационного обмена (далее – Инструкция) разработана в соответствии с руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденным решением председателя Гостехкомиссии от 25.07.1997.

1.2. Настоящая Инструкция определяет основные требования по организации работы в информационных сетях общего пользования и (или) международного информационного обмена, в том числе сети Интернет, (далее – Сеть), порядок обеспечения защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании Сети в ТОГАПОУ «Аграрно-промышленный колледж» (далее – Организация).

1.3. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в Сети.

1.4. Работа в Сети на элементах автоматизированной системы, содержащих конфиденциальную информацию в Организации должна проводиться при служебной необходимости.

2. Основные понятия и сокращения, используемые в настоящей Инструкции

2.1. Абонент информационной сети общего пользования (абонент Сети) – юридическое или физическое лицо, в том числе являющееся сотрудником организации, осуществляющее взаимодействие с Сетью.

2.2. Абонентский пункт (АП) – автоматизированная система, подключаемая к Сети с помощью коммуникационного оборудования и предназначенная для работы абонента Сети.

2.3. Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.4. Администратор защиты информации – лицо, ответственное за защиту АС от несанкционированного доступа к информации.

2.5. Информационная сеть общего пользования (Сеть) – вычислительная (информационно-телекоммуникационная) сеть, открытая для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

2.6. Конфиденциальная информация (КИ) – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

2.7. Локальная вычислительная сеть (ЛВС) – вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования.

2.8. Межсетевой экран (МЭ) – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС.

2.9. Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

3. Порядок подключения абонентского пункта к Сети

3.1. Основные угрозы безопасности информации, возникающие при взаимодействии абонентских пунктов с Сетью:

– несанкционированный доступ к информации, хранящейся и обрабатываемой во внутренних локальных вычислительных сетях (серверах, рабочих станциях) или на автономных ПЭВМ, как из Сетей, так и из внутренних ЛВС;

– несанкционированный доступ к сетевому коммуникационному оборудованию, соединяющему внутренние ЛВС организации с Сетями;

– несанкционированный доступ к данным, передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;

– заражение программного обеспечения вредоносными программами, поступающими из Сети;

- внедрение программных закладок с целью получения несанкционированного доступа к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;

- несанкционированной передачи защищаемой конфиденциальной информации в Сеть;

– возможности перехвата конфиденциальной информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

3.2. Подключение к Сети АП осуществляется по решению руководителя Организации на основании соответствующего обоснования.

3.3. Обоснование необходимости подключения АП к Сети должно содержать:

– наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;

– состав технических средств для оборудования АП;

– предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;

– режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);

– состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети);

– число и перечень предполагаемых абонентов (диапазон используемых IP- адресов);

– меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;

- перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

3.4. Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, конфиденциального характера, разрешается только после установки на АП средств защиты информации от НСД.

4. Порядок изменения состава и конфигурации технических и программных средств АП

4.1. На технических средствах абонентского пункта должно находиться только программное обеспечение, необходимое для функционирования системы.

4.2. При работе технических средств в Сети осуществляется при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

4.3. Все изменения конфигурации технических и программных средств АП должны производиться только на основании заявок сотрудников, имеющих доступ к АП, обусловленный исполнением служебных обязанностей либо администратора защиты информации, согласованных с ответственным за обеспечения безопасности информации.

4.4. Изменение состава и конфигурации технических и программных средств АП производится в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств…».

5. Порядок допуска и регистрации пользователей АП

5.1. Допуск пользователей к работам на АП с определением полномочий пользователя оформляется с санкции руководителя Организации и администратора защиты информации.

5.2. К работе на АП допускаются лица, ознакомленные с требованиями по безопасности информации и настоящей Инструкции.

5.3. Регистрацию пользователей АП производит администратор защиты информации с присвоением каждому пользователю персонального идентификатора (учетной записи) и пароля и назначением определенных прав доступа к ресурсам.

6. Порядок оформления разрешений для пользователей АП на обмен информацией в Сети

6.1. Передача (обмен) информацией по каналам связи осуществляется при использовании защищенных каналов связи, включая доверенные каналы связи, при использовании открытых каналов связи применяются сертифицированные криптографические средства защиты информации.

6.2. Передавать по Сети конфиденциальную информацию без использования средств защиты каналов связи запрещается.

6.3. Пользователь несет личную ответственность за весь информационный обмен между его АП и другими ПЭВМ при работе в Сети.

7. Порядок установки и настройки на АП программного обеспечения, его обновления

7.1. На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном в Организации порядке).

7.2. Установку программного обеспечения, обеспечивающего функционирование АП, должен выполнять только Администратор защиты информации.

7.3. Пользователям не разрешается самостоятельно устанавливать либо изменять настройки программного обеспечения для работы в сети.

7.4. Модификация конфигурации программного обеспечения АП должна производиться только администратором защиты информации.

7.5. Пользователи должны соблюдать условия всех программных лицензий, авторское право и иные федеральные нормативные правовые акты, касающиеся интеллектуальной собственности.

8. Порядок применения средств защиты от НСД на АП и при организации взаимодействия с Сетью

8.1. Для обеспечения защиты информационных ресурсов АП при подключении к Сети необходимо:

– обеспечивать фильтрацию входящих/исходящих сетевых пакетов по правилам, заданным администратором защиты информации;

– скрывать внутреннюю структуру АП;

– осуществлять периодический анализ безопасности установленных МЭ на основе имитации внешних атак на АП;

– осуществлять активный аудит безопасности АП (узлов, сегментов, сетевого оборудования и т.д.) на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

– осуществлять анализ принимаемой из Сети информации, в том числе на наличие вредоносных программ.

8.2. В соответствии с руководящими документами ФСТЭК России, мероприятия по защите конфиденциальной информации при их обработке в АС Организации от НСД, включают в себя:

– организацию управления доступом;

– организацию регистрации и учета;

– обеспечение целостности;

– контроль отсутствия недекларированных возможностей (НДВ);

– антивирусную защиту;

– обеспечение безопасного межсетевого взаимодействия АС;

– анализ защищенности;

– обнаружение вторжений.

8.3. Подключение ЛВС Организации к Сети должно осуществляться через средства разграничения доступа в виде межсетевого экрана (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

8.4. Доступ к МЭ, к средствам его конфигурирования должен осуществляться только администратором защиты информации.

8.5. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП и отвечать требованиям РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

8.6. СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС Организации при обработке на них конфиденциальной информации, должна осуществлять:

– идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;

– контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;

– регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

– регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

8.7. СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

8.8. Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

8.9. В АС, имеющей подключение к Сети или при функционировании которой предусмотрено использование съемных машинных носителей информации, используются средства антивирусной защиты.

9. Порядок работы пользователей с описанием всех разрешенных видов и способов взаимодействия с Сетью

9.1. Работа в Сети на элементах АС, должна проводиться при служебной необходимости

9.2. Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации учитываются в журналах делопроизводства.

9.3. Работа в Сети определяется системой разграничения доступа, запрещающей посторонним лицам доступ к ресурсам АС и позволяющей разграничить права пользователей при работе на АП, при этом контролируются права локальных, удаленных и терминальных пользователей.

9.4. При работе в Сети запрещается:

– подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;

– осуществлять работу в Сети при отключенных средствах защиты информации;

– изменять состав и конфигурацию программных и технических средств АП без санкции администратора защиты информации;

– производить отправку данных без соответствующего разрешения;

– использовать не зарегистрированные в «Журнале учета машинных носителей информации» носители информации;

– нецелевое использование подключения к Сети.

9.5. Пересылка конфиденциальной информации без использования специальных средств защиты по общедоступным Сетям запрещается.

9.6. Цель, методы и содержание работы на АП должны соответствовать должностным обязанностям пользователя АП.

9.7. Пользователю АП запрещается самостоятельно:

– отключать сетевое оборудование общего пользования;

– изменять конфигурацию, производить ремонт АП;

– подключать периферийные устройства, не предусмотренные для конкретного рабочего места;

– устанавливать новое или модифицировать имеющееся системное, офисное, прикладное, сетевое и другие виды программного обеспечения. Необходимость замены (модификации, новой установки и т.п.) программного обеспечения определяется администратором защиты информации.

9.8. Пользователь АП должен знать и уметь пользоваться тем антивирусным программным обеспечением, которое находится на АП. Перед проведением любых операций с внешним носителем информации, в том числе использование носителя для передачи информации по Сети, пользователь АП обязан произвести антивирусную проверку внешнего носителя информации.

9.9. Пользователь АП не имеет право работать от имени другого пользователя АП, осуществлять несанкционированный доступ к информационным ресурсам Сети, ему не предназначенным, предпринимать другие действия, приводящие к незаконному просмотру, копированию, модификации или удалению информационных ресурсов.

9.10. Все информационные материалы, связанные с обеспечением работы Организации, необходимо хранить в специально выделенных местах хранения. Администратор защиты информации осуществляет резервное копирование всех данных на архивный носитель.

9.11. Пользователям АП запрещается хранить на серверах Организации информацию, не связанную с функциональными обязанностями.

10. Обязанности и ответственность пользователей и администратора защиты информации при взаимодействии с Сетью

10.1. Пользователи АП обязаны:

– знать порядок регистрации и взаимодействия в Сети;

– знать инструкцию по обеспечению безопасности информации на АП;

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

– знать и строго выполнять правила работы со средствами защиты информации, установленными на АП (серверах, рабочих станциях АП);

– уметь пользоваться средствами антивирусной защиты;

– после окончания работы в Сети проверить свое рабочее место на наличие вредоносных программ.

10.2. Администратор защиты информации обязан:

– перед работой пользователей в Сети обеспечить обновление антивирусных баз;

– обеспечить выдачу аутентификаторов (имя пользователя/электронный адрес) и идентификаторов (пароль) пользователя, а также регулярную смену идентификаторов;

– после окончания работы проверить технические средства на наличие/отсутствие вредоносного кода и целостность АС (запрещается использование АС при отключенных или неисправных средствах защиты информации).

11. Порядок контроля за выполнением мероприятий по обеспечению защиты информации и работой пользователей

11.1. В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации необходимо:

– осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие вредоносных программ;

– проводить постоянный контроль информации, помещаемой на АП и серверы Организации.

11.2. Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на Администратора защиты информации, руководителей структурных подразделений, определенных в распорядительном документе руководителя Организации.

12. Заключение

12.1. Настоящая Инструкция доводится до абонентов Сети Организации под роспись.

12.2. Настоящая Инструкция вступает в силу с момента её утверждения руководителем Организации.

ЛИСТ

ознакомления с инструкцией по обеспечению безопасности информации при взаимодействии абонентов с информационными сетями общего пользования и (или) сетями международного информационного обмена в ТОГАПОУ «Аграрно-промышленный колледж»

№ п/п	Фамилия, имя, отчество	Должность	Дата	Подпись

Специалист по защите информации В.М.Салычев