МФТИ it
УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Положение
об антивирусной защите информации в МФТИ

1. Общие положения

1.1 Положение о антивирусной защите информации (далее – Положение) определяет требования к организации антивирусной защиты информационных систем (далее – ИС) от воздействий компьютерных вирусов, единый порядок оснащения средствами антивирусной защиты информации, ответственность должностных лиц МФТИ, эксплуатирующих и сопровождающих ИС, за выполнение требований антивирусной защиты, порядок эксплуатации средствами антивирусной защиты информации.

1.2 Положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

2. Требования к организации антивирусной защиты ИС МФТИ от воздействий компьютерных вирусов

2.1 Система антивирусной защиты информации предназначена для предотвращения заражения ИС вредоносными программами, выявления и безопасного удаления их из ИС в случае заражения, предотвращения повреждения информации, обрабатываемой в ИС, предотвращения несанкционированных массовых почтовых рассылок и совершения противоправных действий, которые могут быть осуществлены с персональных компьютеров и серверов МФТИ в случае такого заражения.

2.2 Антивирусная защита информации в МФТИ осуществляется посредством применения организационных мер и средствами антивирусной защиты информации.

2.3 Функционирование системы антивирусной защиты информации осуществляется в рамках единой системы информационной безопасности МФТИ.

2.4 Требования Положения обязательны для выполнения всеми работниками МФТИ.

2.5 Антивирусная защита ИС осуществляется централизованно отделом эксплуатации аппаратных систем и программных средств (далее - ОЭАСПС) УИТ. Для этой цели используется антивирусная программа корпоративного класса (далее - антивирус), имеющая сервер централизованного администрирования (далее - Антивирусный центр) и

программы-агенты для установки на сервера и персональные компьютеры, обеспечивающие централизованный мониторинг и управление антивирусом. Антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники ИС, в том числе из Интернет и с внешних носителей.

2.6 Функционирование средств антивирусной защиты информации осуществляется автоматически в круглосуточном режиме.

3. Единый порядок оснащения средствами антивирусной защиты информации

3.1 Закупка и продление сопровождения (обновление лицензии) средств антивирусной защиты для всех подразделений осуществляется централизованно, за счет средств МФТИ.

3.2 Установка средств антивирусной защиты осуществляется на:

- все персональные рабочие станции пользователей - сотрудников МФТИ, штатных и оформленных по договорам ГПХ;
- рабочие станции школ, кафедр, департаментов, лабораторий и иных подразделений МФТИ, в том числе имеющих собственных системных администраторов;
- все сервера МФТИ, в том числе закреплённые за подразделениями, имеющие собственных системных администраторов;
- почтовые сервера МФТИ.

3.3 На все вышеуказанные средства вычислительной техники в обязательном порядке устанавливается антивирус и агент управления антивирусом, который подключен к Антивирусному центру, что обеспечивает централизованный мониторинг состояния антивирусной защиты, обновление, конфигурирование, периодическую регламентную проверку рабочей станции и серверов.

4. Ответственность должностных лиц за выполнение требований антивирусной защиты

4.1 Ответственным за организацию антивирусной защиты в МФТИ является начальник ОЭАСПС.

4.2 Начальник ОЭАСПС осуществляет организацию и непосредственное руководство проведением работ по антивирусной защите информации в МФТИ. В обязанности начальника ОЭАСПС по обеспечению антивирусной защиты входит:

- разработка положений, инструкций, шаблонов служебных записок (заявок) по задачам организации антивирусной защиты информации;

- определение потребностей, закупка средств антивирусной защиты информации, ежегодное продление лицензий;
- планирование мероприятий по антивирусной защите информации;
- анализ состояния антивирусной защиты информации и разработка предложений о совершенствовании системы антивирусной защиты;
- проведение служебных проверок по фактам заражения компьютерными вирусами автоматизированных систем обработки информации МФТИ.

4.3 За выполнение технических мероприятий по обеспечению антивирусной защиты непосредственно отвечает администратор антивирусной защиты, назначаемый начальником ОЭАСПС из состава системных администраторов ОЭАСПС.

4.4 Администратор антивирусной защиты непосредственно выполняет технические мероприятия по организации антивирусной защиты, определяемые инструкцией администратора антивирусной защиты МФТИ.

4.5 Инструкция администратора антивирусной защиты утверждается начальником УИТ.

4.6 В подразделениях МФТИ, которые не обслуживаются ОЭАСПС и имеют собственных системных администраторов, за исполнение данного положения отвечают руководители этих подразделений. За выполнение технических мероприятий по установке средств антивирусной защиты непосредственно отвечают системные администраторы, назначаемые руководителями этих подразделений.

4.7 Непосредственную ответственность за соблюдение при исполнении обязанностей установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное информирование администратора антивирусной защиты о получении предупреждающих сообщений от установленной антивирусной программы несут пользователи (сотрудники МФТИ) персональных компьютеров. Пользователям, в том числе получившим в установленном порядке права локального системного администратора, запрещается отключать (удалять) антивирусную программу, включая агент удаленного управления антивирусом.

5. Порядок эксплуатации средств антивирусной защиты информации

5.1 Установку средств антивирусной защиты производят системные администраторы ОЭАСПС.

5.2 Установку средств антивирусной защиты в подразделениях МФТИ, имеющих собственных системных администраторов, производят системные администраторы этих подразделений.

5.3 Установку средств антивирусной защиты на физические и виртуальные сервера, подключенные к Интернет, производят их ответственные системные администраторы, определяемые в соответствующей заявке на подключение сервера к Интернет.

5.4 Установку средств антивирусной защиты на почтового сервера производят администраторы этих серверов.

5.5 Порядок установки антивируса, агента управления антивирусом и порядок подключения его к Антивирусному центру определяются администратором антивирусной защиты ОЭАСПС. Инструкция для системных администраторов подразделений по установке средств антивирусной защиты размещена на странице https://mipt.ru/it/documents

5.6 Порядок эксплуатации средств антивирусной защиты информации устанавливается с учетом соблюдения:

- обязательного входного контроля на отсутствие программных вирусов на всех поступающих на объект информатизации электронных носителей информации, в информационных массивах, программных средствах общего и специального назначения;
- обязательной проверки всех электронных писем на предмет отсутствия программных вирусов;
- обязательной проверки используемых в работе съемных носителей информации перед началом работы с ними;
- обязательной еженедельной проверки на предмет отсутствия программных вирусов на жестких магнитных дисках рабочих станций и серверов;
- внеплановой проверки любых носителей информации и средств вычислительной техники в случае подозрения на наличие программных вирусов;
- восстановления работоспособности программных средств и файлов, поврежденных программными вирусами.

5.7 Обновление антивирусных баз на рабочих станциях и серверах МФТИ производится автоматически, ежечасно, с серверов обновления разработчика антивируса или с сервера антивирусной защиты. На рабочих станциях пользователей, не имеющих подключения к локальной сети, подключение к Антивирусному центру не производится, установка, настройка, антивирусных баз осуществляется локально.

5.8 Антивирусный центр должен обеспечивать:

- удалённую установку и обновление средств антивирусной защиты;
- управление конфигурацией всего программного обеспечения системы антивирусной защиты информации;
- управление установкой и обновлением лицензионных ключей антивируса;
- управление установкой обновлений антивирусных баз;

- обеспечение обновления антивирусных баз на рабочих станциях и серверах, подключенных к локальной сети, но не имеющих доступа к Интернет;
- ограничение доступа пользователей на рабочих местах к настройкам антивируса;
- настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе антивируса и т.п.;
- удаленное решение проблем, возникающих в процессе эксплуатации средств антивирусной защиты информации;
- иметь в составе средства мониторинга и отчетности о состоянии антивирусной защиты.