«УТВЕРЖДЕНО»
приказом №_____ от «____» _____2013г

ПРАВИЛА

использования информационных систем и ИТ-сервисов ТГУ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие правила разработаны с целью установить единые требования к пользователям компьютеров в области информационной безопасности.

1.2. Настоящие правила определяют требования к работе с информационными системами, сервисами и средствами обработки и хранения информации.

2. ОБЩИЕ ТРЕБОВАНИЯ

2.1. Пользователю запрещается:

2.1.1. Использовать в работе и самостоятельно устанавливать нелицензионное программное обеспечение (ПО)

2.1.2. Самовольно вносить изменения в комплектацию компьютеров и их конфигурацию

2.1.3. Перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ЦНИТ

2.1.4. Самостоятельно повышать свои привилегии в операционной системе

2.1.5. Оставлять без личного присмотра на рабочем месте или где бы то ни было носители ключевой информации

2.1.6. Подключать к компьютеру, на котором обрабатывается информация конфиденциального характера личные мобильные устройства (ноутбуки, нетбуки, планшеты, смартфоны, за исключением зарегистрированных в отделе собственной безопасности) и личное сетевое оборудование (маршрутизаторы, концентраторы, Wi-Fi-роутеры) к корпоративной информационной сети (выполнение требований приказа ФСЭК № 21 для информационных систем 4-го уровня защиты (15. Ограничение и контроль использования мобильных устройств, носителей информации)

2.1.7. Копировать информацию конфиденциального характера на неучтенные в ОСБ внешние носители (флешки,CD)

2.1.8. Использовать бесплатные почтовые сервисы (mail.ru, yandex.ru,gmail.com и пр.) для обмена электронными сообщениями, содержащими конфиденциальные данные (перечень информации конфиденциального характера определен приказом ректора № 3670 от 27.08.2010 «Об утверждении перечня сведений конфиденциального характера»)

2.1.9. Пересылать конфиденциальные данные при помощи сервисов мгновенных сообщений (ICQ, Jabber и др.)

2.1.10. Использовать информационные ресурсы университета для участия в сетевых играх, распространения коммерческой рекламы, организации СПАМа и.т.п.

2.1.11. Отключать функцию автоматического обновления операционной системы.

3. РАБОТА В СЕТИ ИНТЕРНЕТ

3.1. При пользовании интернетом запрещается:

3.1.1. Передавать информацию конфиденциального характера через Интернет
3.1.2. Разглашать информацию конфиденциального характера в социальных сетях, интернет-форумах и блогах
3.1.3. Использовать пароли, используемые во внутренней сети, при регистрации на Интернет-серверах
3.1.4. Посещать сайты экстремистского и порнографического содержания
3.1.5. Переходить по ссылкам, запускающим на выполнение исполняемые или командные файлы
3.1.6. Самостоятельно скачивать и устанавливать любое программное обеспечение.

4. АНТИВИРУСНАЯ ЗАЩИТА

4.1. В целях предотвращения заражения компьютерным вирусом запрещается:

4.1.1. Открывать вложения в письмах, полученных от неизвестного источника
4.1.2. Копировать информацию с внешних носителей без предварительной проверки
4.1.3. Переходить по Интернет ссылкам, указанным в письмах от неизвестного источника и письмах рекламного характера
4.1.4. Отключать защиту или приостанавливать работу антивирусной программы

4.2. При появлении сообщения об окончании лицензии на использование антивирусного ПО необходимо немедленно подать заявку в ЦНИТ на обновление ключа программы.

4.3. Признаками того, что компьютер заражен вредоносными программами, может быть снижение производительности, появление всплывающих окон, несанкционированное изменение домашней страницы, постоянные предупреждения брандмауэра и т.д. В случае возникновения вышеуказанных проблем прекратить работу за компьютером и подать заявку в ЦНИТ на устранение вирусного заражения.

5. ЭЛЕКТРОННАЯ ПОЧТА

5.1. При пользовании электронной почтой запрещается:

5.1.1. Открывать электронные письма, полученные от неизвестных источников
5.1.2. Принимать электронные открытки от неизвестных лиц
5.1.3. Открывать письма с заведомым спамом
5.1.4. Разглашать свой адрес электронной почты на интернет-ресурсах
5.1.5. Распространять материалы, использование и распространение которых ограничено действующим законодательством РФ.

6. ПАРОЛЬНАЯ ЗАЩИТА

6.1. Пользователям для локального входа в операционную систему рекомендуется использовать логин/пароль

6.2. Не рекомендуется использовать один и тот же логин/пароль для доступа к различным ресурсам

6.3. Не допускается длина пароля менее 6 буквенно-цифровых символов

6.4. Не допускается хранить пароли в браузерах. Современные браузеры не обеспечивают надежную защиту учетных данных. При необходимости рекомендуется использовать специализированные менеджеры паролей

6.5. При компрометации полученного пароля необходимо подать заявку администратору соответствующей информационной системы для смены пароля

6.6. В случае заражения компьютерными вирусами типа BackDoor (крадущими идентификационные данные) должны быть приняты меры к изменению всех паролей.

7. ХРАНЕНИЕ И РЕЗЕРВИРОВАНИЕ ИНФОРМАЦИИ

7.1. Не рекомендуется хранить созданные файлы на рабочем столе или системном разделе диска

7.2. Для обмена данными рекомендуется использовать файлообменники. В случае использования общих ресурсов не допускается хранение информации конфиденциального характера в папках с общим доступом

7.3. Важная информация подлежит архивированию и хранению. Отчуждаемые носители для хранения резервных копий информации конфиденциального характера, используемые администраторами информационных систем, должны быть зарегистрированы в отделе собственной безопасности

7.4. В случае потери информации в результате сбоев системы или вирусной атаки самостоятельно не предпринимать никаких действий, подать заявку в ЦНИТ на восстановление информации или системы.

8. УДАЛЕННЫЙ ДОСТУП К КОРПОРАТИВНОЙ СЕТИ

8.1. Не допускается установка и использование пакетов программного обеспечения для удалённого контроля компьютеров

8.2. Удаленный доступ возможен только на ограниченное время по служебной записке на имя директора ЦНИТ с подробным обоснованием необходимости доступа

8.3. Не допускается несанкционированная установка роутеров WiFi.

9. ИСПОЛЬЗОВАНИЕ СИСТЕМ МОНИТОРИНГА

9.1 В целях предотвращения утечек информации и разбора возникающих инцидентов нарушения информационной безопасности на серверах, межсетевых экранах, встроенными системами журналирования в информационных системах отделом собственной безопасности ведется аудит действий пользователей в корпоративной сети, сети интернет, в информационных системах

9.2 В контролируемых зонах университета в режиме реального времени ведется видеонаблюдение.

5. Список разработчиков и согласования

Список разработчиков:

Главный специалист по ИБ И.А. Власов

Начальник

Отдела собственной безопасности В.В. Басацкий

Список согласования:

Проректор по безопасности Б.И. Сидлер

Директор ЦНИТ В.В. Ефросинин