УТВЕРЖДЕНО
приказом №_____ от _____2011

ПОРЯДОК

действий пользователя информационной системы по обеспечению информационной безопасности в Тольяттинском государственном университете

СОГЛАСОВАНО
Проректор по безопасности
_____Б.И. Сидлер
«____»_____2011 г.

Тольятти 2011

СОДЕРЖАНИЕ

1. Область применения

Настоящий порядок предназначен для сотрудников Тольяттинского государственного университета (ТГУ). Он регулирует порядок допуска пользователей к работе в локальной вычислительной сети, а также определяет правила обращения с защищаемой информацией, обрабатываемой, хранимой и передаваемой в пределах локальной вычислительной сети Университета.

2.Обозначения и сокращения

АВС – антивирусные средства

ИС – информационная система

ИБ – информационная безопасность

ОСБ – отдел собственной безопасности

ЛВС – локальная вычислительная сеть

НСД – несанкционированный доступ

SD – ServisDesk

ПДн – персональные данные

ИСПДн – информационная система, обрабатывающая персональные данные

ПО – программное обеспечение

Университет – ФГБОУ ВПО «Тольяттинский государственный университет».

3. Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи ИБ сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких действий.

4. Основные положения

Обеспечение ИБ направлено на достижение:

- конфиденциальности – предотвращение утечек информации;
- целостности – защита информации от неавторизованных изменений и вмешательств в работу информационных систем;
- доступности – обеспечение доступа авторизованных пользователей к информации, согласно предоставленных прав;
- обеспечение уверенности, что информация защищена от хищения, уничтожения, НСД, искажения.

5. Общие принципы защиты

Не допускается проведение пользователем сетевых атак и сетевого взлома, а так же участия в них. Под сетевой атакой понимаются действия, направленные на получение НСД к ресурсу ЛВС, а так же умышленное уничтожение ПО или данных, не принадлежащих пользователю, под НСД понимается любой доступ, полученный способом, отличным от описанного в настоящем порядке.

Пользователю запрещены:

1. Действия, направленные на нарушение нормального функционирования элементов ЛВС (компьютеров, другого оборудования или ПО);
2. Целенаправленные действия по сканированию узлов сетей с целью выявления внутренней структуры ЛВС;
3. Использование в работе и самостоятельная установка нелицензионного ПО и драйверов устройств;
4. Самовольное внесение изменений в устройство и конфигурацию компьютеров;
5. Допуск посторонних лиц к своей рабочей станции (компьютер) или осуществление обработки информации конфиденциального характера в их присутствии;
6. Оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
7. Оставлять без личного присмотра на рабочем месте или где бы то ни было носители ключевой информации;
8. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям информационной безопасности и возникновению кризисной ситуации. При обнаружении такого рода ошибок пользователь обязан ставить в известность сотрудника ОСБ и руководителя своего подразделения;
9. Копирование информации на неучтенные внешние носители.

6. Предоставление доступа к работе в ЛВС

Руководитель структурного подразделения, в котором работает пользователь, оформляет заявку в произвольной форме на предоставление доступа к ИС на имя одного из должностных лиц, определенных в приказе № 56300 от 27.11.2008 "О наделении должностных лиц правом подписи документов", или директора ЦНИТ. В заявке определяются права и роль пользователя, разделы информации, на которые распространяется доступ, срок начала действия доступа.

Устные запросы сотрудников на предоставление доступа не рассматриваются.

Пользователям выдаются логины и пароли для доступа к ИС согласно порядка предоставления доступа.

7. Использование ресурсов ЛВС для хранения и обмена данных между пользователями

В отдельных ИС или рабочих группах, доменах, администраторы ИС создают файловые обменники, с персональными каталогами пользователей, через которые пользователи рабочей группы обмениваются неконфидециальной информацией. Данные пользователей также могут быть размещены на файловом сервере, они подлежат резервному копированию. Документы, хранящиеся на компьютерах пользователей не синхронизируются с файловым сервером и не подлежат резервному копированию. За сохранность данных на локальном компьютере ответственность несет сотрудник.

Отдельные программы для совместной работы пользователей требуют подключения сетевого диска с указанием пути к общему ресурсу на компьютере, выполняющему роль сервера. Такой тип подключения организуется по служебной записке на имя директора ЦНИТ, с регистрацией заявки через SD.

8. Требования к выбору и использованию пароля доступа

При выборе, использовании и смене пароля пользователь обязан руководствоваться документом «Порядок выдачи и смены паролей для доступа к информационным системам ТГУ» (утвержден приказом ректора от 30.06.2011 №3024).

9. Порядок установки дополнительного ПО

Пользователю запрещается самостоятельно устанавливать и удалять программное обеспечение.

9.1 Для пользователей АУП, АХЧ

При необходимости установки дополнительного ПО пользователь должен согласовать свое решение с руководителем подразделения и обратиться в ЦНИТ со служебной запиской.

Порядок установки:

- руководитель структурного подразделения подает служебную записку на имя директора ЦНИТ с обоснованием необходимости установки данного ПО пользователю.
- в случаях, перечисленных выше сотрудник отдела ИБ дает заключение по поводу установки и делает свою пометку в служебной записке;
- сотрудник ЦНИТ производит установку ПО на основании служебной записки.

В случае сбоев в работе установленного ПО пользователь должен обратиться в Службу поддержки пользователей (Service Desk) по тел. 53-91-39.

9.2 Для пользователей учебных подразделений

При необходимости установки дополнительного ПО, пользователь должен согласовать свое решение с руководителем подразделения, после чего самостоятельно или с привлечением ИТ-специалистов учебного подразделения осуществить установку необходимого ПО.

В случае сбоев в работе установленного ПО пользователь должен обратиться к ИТ-специалисту учебного подразделения или подать заявку в ЦНИТ через SD.

ЦНИТ осуществляет постоянный мониторинг установленного программного обеспечения на персональных компьютерах пользователей. В случае установки нелицензионного ПО или установки ПО без ведома руководителя подразделения, сотрудники ЦНИТ удаляют ПО и ставят в известность руководителя о нарушении порядка.

10. Требования по работе в сети Интернет

Логин и пароль для электронной почты пользователь получает у системного администратора ЦНИТ на основании заявки.

Основные требования при работе в сети Интернет:

- запрещается передавать конфиденциальную информацию через Интернет без использования специальных каналов;
- запрещается использовать пароли, используемые во внутренней сети при регистрации на Интернет-серверах;
- запрещается пользование бесплатными почтовыми серверами для пересылки конфиденциальной информации или ПДн;
- запрещается посещение сайтов сомнительного содержания ввиду возможной блокировки компьютера;
- запрещается разглашать конфиденциальную информацию или информацию, содержащую ПДн через социальные сети, ISQ, QIP и.т.д.;

Действия любого пользователя не соблюдающего данные правила будут запротоколированы, информация по нарушениям подобного характера будет передана в ОСБ для разбирательства.

11. Требования к обеспечению антивирусной защиты

На все компьютеры сети установлены антивирусные пакеты, антивирусные базы регулярно обновляются в автоматическом режиме без участия пользователя.

Все данные с внешних носителей, из электронной почты, из сети Интернет должны быть проверены на вирусы.

В случае необычного поведения компьютера (замедление работы, непроизвольные перезагрузки, зависания) необходимо сообщить ответственному сотруднику ЦНИТ через SD.

Источниками компьютерных вирусов могут быть:

- сайты сомнительного содержания;
- почтовые вложения;
- внешние носители данных;
- скаченное из Интернета ПО.

В целях защиты от вирусов пользователям запрещается:

- открывать вложения в письмах, полученных от неизвестного источника;
- забирать информацию с внешних носителей без предварительной проверки;
- следовать по Интернет ссылкам, указанным в письмах от неизвестного источника и письмах рекламного характера;
- отключать или приостанавливать антивирусную защиту.

12. Требования к обеспечению защиты персональных данных

Все сотрудники Университета, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Пользователь ИСПДн обязан:

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;
- выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в «Положении о разграничении прав доступа к обрабатываемым персональным данным»;
- знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов;
- обо всех выявленных нарушениях, связанных с информационной безопасностью Университета, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться в главный корпус университета в 215 кабинет, по электронной почте Vlas@tltsu.ru или по внутреннему телефону 53-95-62, к сотруднику по информационной безопасности ОСБ.

Пользователю ИСПДн запрещается:

- разглашать защищаемую информацию, определенную в «Перечне объектов ИСПДн Университета, подлежащих защите», третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с ответственным за обеспечение защиты персональных данных.

Сотрудник должен быть ознакомлен с Положением «Об обработке персональных данных» под подпись.

Приложение

С требованиями порядка действий пользователя информационной системы по обеспечению информационной безопасности в ТГУ ознакомлен и обязуюсь их выполнять

Сотрудник подразделения _____ / _____

Руководитель подразделения _____ / _____

< _____>_____201_г.