Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Мордовский государственный университет им. Н. П. Огарева»

Факультет математики и информационных технологий

ЛАБОРАТОРНАЯ РАБОТА № 2

«Политика информационной безопасности на ТЭЦ»

Выполнил:

студент 402 группы

Батунин М. Е.

Саранск 2018

**Общие положения**

Информация является ценным и жизненно важным ресурсом ТЭЦ (далее – Компания). Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Компании.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании, при этом первоочередной задачей является обеспечение безопасности всех активов Компании. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Компании. Главные цели Компании не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящей Политике под термином "сотрудник" понимаются все сотрудники Компании. На лиц, работающих в Компании по договорам гражданско-правового характера, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

Целями настоящей Политики являются:

* сохранение конфиденциальности критичных информационных ресурсов;
* обеспечение непрерывности доступа к информационным ресурсам Компании для поддержки бизнес деятельности;
* защита целостности деловой информации с целью поддержания возможности Компании по оказанию услуг высокого качества и принятию эффективных управленческих решений;
* повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Компании;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Компании.

Руководители подразделений Компании должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки Руководству.

**Область применения настоящей Политики**

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Компании. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Компании, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

Компании принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Компании, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Компании.

**Контроль доступа к информационным системам**

**Общие положения**

Все работы в пределах офисов Компании выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Компании.

Внос в здания и помещения Компании личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Компании производится только при согласовании с Отделом защиты информации Компании.

Все данные (конфиденциальные или строго конфиденциальные), составляющие коммерческую тайну Компании и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Компании должны быть оснащены программным обеспечением по шифрованию жесткого диска.

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования.

Доступ третьих лиц к информационным системам Компании должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Компании должен быть четко определен, контролируем и защищен.

**Доступ к сети Интернет**

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

**Рекомендованные правила:**

* сотрудникам Компании разрешается использовать сеть Интернет только в служебных целях;
* сотрудники Компании не должны использовать сеть Интернет для хранения корпоративных данных;
* сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Компании;
* запрещен доступ в Интернет через сеть Компании для всех лиц, не являющихся сотрудниками Компании.

Специалисты Отдела информационных технологий и Отдела защиты информации имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

**Защита оборудования**

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, используемого в процессе работы

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты Отдела информационных технологий, после согласования изменений с Отдела защиты информации.

**Аппаратное обеспечение**

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное Компанией, является ее собственностью и предназначено для использования исключительно в производственных целях.

Все компьютеры должны защищаться паролем при загрузке системы. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией для всех компонентов оборудования, в состав которых входят носители данных должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

**Программное обеспечение**

Все программное обеспечение, установленное на предоставленном Компанией компьютерном и производственном оборудовании, является собственностью Компании и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование оборудовании нестандартное или программное обеспечение, не имеющее отношения к их производственной деятельности.

На всех корпоративных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

* персональный межсетевой экран;
* антивирусное программное обеспечение;
* программное обеспечение шифрования жестких дисков;
* программное обеспечение шифрования почтовых сообщений.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем Отдела информационных технологий.

Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

**Управление сетью**

Уполномоченные сотрудники Отдела информационных технологий и Отдела защиты информации контролируют содержание всех потоков данных проходящих через сеть Компании.

Сотрудникам Компании запрещается:

* нарушать информационную безопасность и работу сети Компании;
* сканировать порты или систему безопасности;
* контролировать работу сети с перехватом данных;
* получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
* использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
* передавать информацию о сотрудниках или списки сотрудников Компании посторонним лицам;
* создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

**Защита и сохранность данных**

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Специалисты Отдела информационных технологий обязаны оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

Все заявки на проведение технического обслуживания компьютеров и оборудования должны направляться в Отдел информационных технологий.