Государственное унитарное предприятие Самарской области
«Экология»

ПАМЯТКА
по безопасной работе сотрудников ГУП «Экология» при использовании сети Интернет

1. Общие положения

1.1. Настоящая Памятка по безопасной работе сотрудников ГУП «Экология» при использовании сети Интернет (далее - Памятка) основана на требованиях Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», нормативных правовых актах Российской Федерации, регулирующих отношения в области защиты информации.
1.2. Целями Памятки являются:
- регулирование работы сотрудников предприятия при использовании сети Интернет;
- обеспечение целостности, конфиденциальности и доступности хранящейся и передаваемой информации, находящейся на автоматизированных рабочих местах (далее – АРМ) или локальной вычислительной сети (далее – ЛВС);
- соблюдение требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области защиты информации.
1.3. При работе в сети Интернет и информационных системах пользователи руководствуются законодательством Российской Федерации, нормативными правовыми актами, иными документами в области информационных технологий и безопасности информации, а также настоящей Памяткой.

2. Общие правила пользования на АРМ

2.1. Пользователь отвечает за правильность включения (выключения) АРМ, вход в систему и все действия при работе на нем.
2.2. АРМ разрешается использовать исключительно в рабочих целях.
2.3. Пользователь обязан исключить возможность неосторожного причинения вреда техническим и информационным ресурсам.
2.4. Систематически осуществлять резервное копирование важной информации, хранящейся на АРМ пользователя.
2.5. Систематически проверять обновление антивирусной базы (как правило, в настройках антивируса, установлено их автоматическое обновление).
2.6. Во время работы экран монитора компьютера располагать в помещении таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами.
2.7. При временном отсутствии пользователя на рабочем месте экран монитора должен быть потушен или использована экранная заставка.
2.8. Соблюдать требования парольной политики (Раздел 6 Памятки).
2.9. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к главному специалисту по ИТ предприятия.
2.10. Использовать электронную подпись (далее – ЭП) в соответствии с Руководством (правилам) по обеспечению использования ЭП и средств ЭП, выданным удостоверяющим центром.
Пользователям запрещается:
2.11. Открывать на АРМ файлы и запускать программы, полученные из непроверенных источников.
2.12. Передавать свои идентификационные данные (пароли, логины), атрибуты доступа к ресурсам информационной системы посторонним лицам.

2.13. Отключать (блокировать) средства защиты информации.
2.14. Привлекать посторонних лиц для производства ремонта или настройки АРМ.
2.15. Разглашать обрабатываемую информацию третьим лицам.
2.16. Копировать информацию на внешние носители без разрешения руководства.
2.17. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
2.18. Несанкционированно открывать общий доступ к папкам на АРМ.
2.19. Осуществлять подключение к АРМ и ЛВС посторонних и личных устройств (например: смартфоны, телефоны, считыватели информации, излучающие устройства (Wi-Fi, Bluetooth, радиомодемы) и т.п.).

3. Правила пользования в сети Интернет

3.1. Ресурсы сети Интернет предоставляются пользователям для получения информации необходимой для выполнения должностных обязанностей.
3.2. Пользователь обязан не предпринимать попыток несанкционированного доступа к информационным ресурсам, доступ к которым ему ограничен.
3.3. Пользователь может посещать только те ресурсы, содержание которых не противоречит законодательству Российской Федерации, а цель посещения должна быть связана с его должностной деятельностью.
3.4. Внимательно набирать имена сайтов, особенно на которых проводятся финансовые операции. Поддельные сайты могут иметь отличие даже одного знака или тот же вид, что и оригинальные. Такие сайты могут содержать невидимые области, нажатие на которые может привести к заражению АРМ вредоносными программами или перенаправление на зараженные сайты. Более безопасно не набирать вручную наименование сайта, а пользоваться заранее сделанными закладками.
3.5. На не проверенных сайтах ввод конфиденциальных данных запрещается.
3.6. Категорически запрещено использование для должностной деятельности иностранных Интернет-сервисов систем обмена сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Viber, Whatsap, Skype, Trello и т.д.), облачных сервисов хранения информации (iCloud, Google Drive, Dropbox и т.д.).
3.7. Пользователям запрещается:
- использовать доступ к сети Интернет в личных целях;
- посещать досугово-развлекательные сайты;
- использовать доступ к сети Интернет для распространения и тиражирования информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

4. Правила работы с электронной почтой

4.1. При получении электронного письма с вложением необходимо внимательно посмотреть адрес отправителя. В случае, если этот адрес неизвестен, или отличается от реального хотя бы одним знаком, открытие вложений таких писем не безопасно, поскольку могут содержать вредоносные программы.
4.2. При получении письма от неизвестного адресата, необходимо связаться с исполнителем и уточнить происхождение файлов. В случае невозможности установить происхождение письма, необходимо его удалить, не сохраняя и не запуская приложенные файлы.
4.3. Запрещается передавать информацию ограниченного доступа через сеть Интернет (в том числе посредством электронной почты) без использования средств защиты информации.
4.4. Запрещается осуществлять массовые рассылки электронной почты несвязанной с должностными обязанностями (СПАМа).
4.5. Необходимо своевременно очищать свой почтовый ящик.

5. Правила антивирусной защиты

5.1. Для обеспечения антивирусной защиты используется сертифицированное лицензионное антивирусное программное обеспечение.
5.2. Пользователи при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
5.3. Обновление антивирусной программы производится автоматически.
5.4. Периодическое тестирование всего установленного программного обеспечения на предмет компьютерных вирусов производится автоматически. Полную проверку АРМ необходимо проводить при установке антивирусной программы, в случаях подозрения заражением, периодически 1 – 2 раза в год.
5.5. В случае обнаружения подозрительных программ срабатывает антивирус и необходимо прекратить какие-либо действия на АРМ и обратиться к главному специалисту по ИТ предприятия.
5.6. В случае обнаружения вируса, не поддающегося лечению, главный специалист по ИТ предприятия, принимает меры по восстановлению работы системы.
5.7. В тех случаях, когда заражение вирусом АРМ все-таки произошло, необходимо:
- немедленно отключить компьютер для остановки действий вредоносной программы и не включать компьютер с зашифрованными данными, т.к. во время включений и перезагрузок происходят изменения файловой системы компьютера;
- не пытаться самостоятельно изменять расширения зараженных файлов, а также удалять любые файлы с рабочего компьютера и электронные сообщения;
- обратиться к главному специалисту по ИТ предприятия;
- обратиться в службу технической поддержки установленной антивирусной программы и совместно с ними попытаться восстановить утраченную информацию.

6. Парольная политика

6.1. Идентификация и проверка подлинности пользователя при входе в АРМ, информационную систему может осуществляться по паролю условно-постоянного действия, с использованием аппаратных средств (TouchMemory и др.), с использованием ЭП.
6.2. Полная плановая смена паролей пользователей должна проводиться регулярно (не реже 1 раза в 3 месяца).
6.3. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.
6.4. В случае компрометации (утраты, разглашения, кражи, взлома) личного пароля, пользователь должен немедленно предпринять меры по смене пароля.
6.5. Хранение пользователем значений своих паролей на материальном носителе допускается только в личном, запираемом ящике (сейфе).
6.6. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).
6.7. Правила формирования пароля:
6.7.1. Пароль должен состоять не менее чем из восьми символов.
6.7.2. В пароле должны присутствовать символы трех категорий из числа следующих четырех:
- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например: !,$,#, %).
6.7.3. Пароль не может содержать имя учетной записи Пользователя или какую-либо его часть.
6.7.4. Пароль не должен включать в себя легко вычисляемые сочетания символов, простые пароли типа «123», «111», «qwerty» и им подобные, а так же ФИО и даты рождения свои и своих

родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые могут быть подобраны, основываясь на информации о пользователе.
6.7.5. Не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «аааааааа»).
6.7.6. Не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).
6.7.7. Не использовать ранее использованные пароли.
6.7.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.
6.7.9. Во время ввода пароля необходимо убедиться, что клавиатура находится вне поля зрения посторонних лиц, а также технических средств (видеокамер, фотоаппаратов).
6.7.10. Не использовать один пароль в разных информационных ресурсах.

7. Ответственность Пользователя

Пользователи несут персональную ответственность за свои действия в период осуществления информационного взаимодействия с использованием АРМ;
За нарушение настоящий Памятки, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, АРМ пользователя может быть отключен от ЛВС до выяснения обстоятельств нарушения.
Нарушение требований законодательства Российской Федерации об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.