ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ ГИМНАЗИЯ № 1
ГОРОДА НОВОКУЙБЫШЕВСКА
ГОРОДСКОГО ОКРУГА НОВОКУЙБЫШЕВСК САМАРСКОЙ ОБЛАСТИ
(ГБОУ гимназия № 1 г. Новокуйбышевска)

446201, Новокуйбышевск, ул. Ворошилова 12, тел. 9-95-05, 5-36-46. E-mail: school16@bk.ru

УТВЕРЖДЕНО
приказом ГБОУгимназии№1
г. Новокуйбышевска
от «20» марта.2017 г. № 118-од
Директор
Л.Г. Слепцова

ПРАВИЛА
по безопасной работе сотрудников при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем

1. Общие положения

1.1. Настоящие Правила по безопасной работе сотрудников при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем (далее – Правила, пользователи) в государственном бюджетном города Новокуйбышевска городского округа Новокуйбышевск Самарской области (далее – образовательная организация) разработаны для:

- регулирования работы пользователей при использовании сети Интернет и осуществлении информационного взаимодействия с сервисами государственных информационных систем;
- обеспечения целостности, конфиденциальности и доступности хранящейся и передаваемой информации, находящейся на автоматизированных рабочих местах (далее – АРМ) или локальной вычислительной сети (далее – ЛВС);
- соблюдения требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области защиты информации.

1.2. Настоящие Правила разработаны в соответствии с:

- Федеральным законом от 29 декабря 2012 г. N 273-ФЗ "Об образовании в Российской Федерации;
- рекомендациями решения Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 27.04.2016 г.;
- письмом министерства образования и науки Самарской области, департамента по надзору и контролю в сфере образования и информационной безопасности от 15 марта 2017 г. № 87-Ник.

1.3. Правила основаны 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.

1.4. 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 Правилами.

1.5. Допуск пользователей для работы в сети Интернет осуществляется в соответствии с нормативно правовыми актами образовательной

организации:

- Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, музейным фондам, материально-техническим средствам обеспечения образовательной деятельности;
- Регламент работы участников образовательных отношений в сети Интернет.

Тезаурус:

- АРМ - автоматизированные рабочие места (далее – АРМ);
- ЛВС- локальные вычислительные сети (далее – ЛВС).

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 служебных 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, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

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 Правил).

2.9. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к специалистам по информационной безопасности.

2.10. Пользователям запрещается:

- открывать на АРМ файлы и запускать программы, полученные из непроверенных источников;
- передавать свои идентификационные данные (пароли, логины),

атрибуты доступа к ресурсам информационной системы посторонним лицам;

- отключать (блокировать) средства защиты информации;
- привлекать посторонних лиц для производства ремонта или настройки АРМ;
- разглашать обрабатываемую информацию третьим лицам;
- копировать служебную информацию на внешние носители без разрешения руководства;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на АРМ;
- 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 служебных 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 служебной деятельностью.

3.4. Внимательно набирать имена сайтов. 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. Категорически запрещено использование для служебной деятельности иностранных Интернет-сервисов систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Viber, Whatsap, Skype и т.д.), облачных сервисов хранения информации (iCloud,

Google Drive, Dropbox и т.д.).
3.6. 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. Для служебной деятельности необходимо использовать электронную почту доменов Российской Федерации. **Категорически запрещено использование иностранных почтовых сервисов электронной почты** (Gmail, Yahoo и т.д.) для служебной деятельности.
4.2. 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.
4.3. При получении письма от неизвестного адресата, необходимо его удалить, не сохраняя и не запуская приложенные файлы.
4.4. Запрещается осуществлять массовые рассылки электронной почты неслужебного характера (СПАМа).
4.5. Необходимо своевременно очищать свой почтовый ящик.

5. Правила антивирусной защиты

5.1. Для обеспечения антивирусной защиты должно использоваться сертифицированное лицензионное антивирусное программное обеспечение.
5.2. Ярлык антивирусной программы, как правило, находится в области уведомления или на вкладке «отображать скрытые значки» (нижний правый угол экрана).
5.3. Пользователи при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
5.4. Обновление антивирусной программы, как правило, производится автоматически, в противном случае необходимо обратиться к

администратору.

5.5. 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.

5.6. В случае обнаружения подозрительных программ срабатывает антивирус и необходимо прекратить какие-либо действия на АРМ и обратиться к администратору.

5.7. В случае обнаружения вируса, не поддающегося лечению, ответственный за обеспечение безопасности информации, принимает меры по восстановлению работы системы.

5.8. Вирусы-шифровальщики не определяются антивирусными программами в момент заражения АРМ.

5.9. 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 должностному лицу, отвечающему за установку антивирусных программ, обеспечение безопасности информации.

По информации производителей антивирусных программ возможность восстановления информации – минимальна, т.к. каждое вредоносное сообщение содержит индивидуальный файл-шифровальщик.

Напоминаем о необходимости проведения регулярной процедуры резервного копирования всей важной рабочей информации АРМ, т.к. это позволит быстро восстановить Ваши данные в случае их повреждения (заражения)!

6. Парольная политика

6.1. Идентификация и проверка подлинности пользователя при входе в АРМ, информационную систему может осуществляться по паролю условно-постоянного действия.

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. 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.).

6.6. Правила формирования пароля:

6.6.1. Пароль должен состоять не менее чем из восьми символов.

6.6.2. 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: !,$,#, %).

6.6.3. Пароль не может содержать имя учетной записи Пользователя или какую-либо его часть.

6.6.4. 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.

6.6.5. Не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «аааааааа»).

6.6.6. Не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

6.6.7. Не использовать ранее использованные пароли.

6.6.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

6.6.9. Во время ввода пароля необходимо убедиться, что клавиатура находится вне поля зрения посторонних лиц, а также технических средств (видеокамер, фотоаппаратов).
6.6.10. 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 настоящих Правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы 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.