«СОГЛАСОВАНО»:
Председатель выборного
органа первичной
профсоюзной организации
ГБОУ СО «Гимназия № 1
(Базовая школа РАН)»
_____ / М.З. Шивани

«УТВЕРЖДАЮ»:
Директор
ГБОУ СО «Гимназия № 1
(Базовая школа РАН)»
_____Л.Е. Загребова
Приказ № /од от

ЭП
O="ГБОУ СО ""
Гимназия №1
(Базовая школа
РАН)""",
CN=Загребова Л.Е.,
E=gymnasia1@mail.r
u
00d52bb22ea5ebd191
2023.02.01
09:11:32+04'00'

СВОД ПРАВИЛ
по безопасной работе сотрудников ГБОУ СО «Гимназия № 1 (Базовая школа РАН)» при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем

1. Общие положения

1.1. Настоящий Свод правил по безопасной работе сотрудников ГБОУ СО «Гимназия № 1 (Базовая школа РАН)» при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем (далее – Свод правил, пользователи) основан 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 областизащиты информации.

1.2. Целями Свода правил являются:

– регулирование работы пользователей при использовании сети Интернет и осуществлении информационного взаимодействия с сервисами государственных информационных систем;

– 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 Сводом правил.

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, не связанной с обучением детей, экран монитора компьютера располагать в помещении таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами. При работе со служебной, персональной, конфиденциальной информацией 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 8 Свода правил).

2.9. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к администратору информационной сети и (или) инженеру.

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 служебную 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 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, 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. В настоящее время киберпреступники создают поддельные сайты якобы для оплаты штрафов ГИБДД или оформления заявки на кредит и других целей. На не проверенных сайтах ввод конфиденциальных данных не рекомендуется!
3.6. Категорически запрещено использование для служебной деятельности иностранных Интернет-сервисов систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Whatsap, Skype и т.д.), облачных сервисов хранения информации (iCloud, Dropbox и т.д.).
3.7. Пользователям запрещается:

– использовать доступ к сети Интернет в личных целях;

– посещать досугово-развлекательные сайты не связанные с образовательным процессом;

– 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 домена Лицея (samlit.info) **Использование иных общедоступных почтовых сервисовдолжно быть исключено**. Используя общедоступные почтовые сервисы Вы **сознательно** предоставляете передаваемую информацию этим сервисам, и она может быть доступна третьим лицам. **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. В последнее время зафиксирована рассылка на электронные адреса пользователей, а также на официальные почтовые ящики органов исполнительной власти Самарской области и органов местного самоуправления муниципальных образований в Самарской области, во вложении к которым содержатся вредоносные файлы типа «Акты сверки.zip», «Коммерческое предложение.zip», «Судебное производство.zip», с различными графическими изображениями. Такие вложения, как правило, содержат вирусы- шифровальщики (Trojan.Encoder), которые имитируют зависание операционной системы Windows компьютера и шифруют документы пользователей с расширениями *.doc, *.xls, *.pdf, *.txt, *.jpg, *.tif, *.rar, *.zip и другими, некоторые передают (воруют) информацию насторонние сервера.

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

4.4. 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.

4.5. Запрещается передавать информацию ограниченного доступа через сеть Интернет (в том числе посредством электронной почты) без использования средств защиты информации.

4.6. Запрещается осуществлять массовые рассылки электронной почты неслужебного характера (СПАМа).

4.7. Необходимо своевременно очищать свой почтовый ящик.

4.8. Необходимо осуществлять ежедневную обработку писем.

5. Правила пользования государственными и муниципальными информационными системами

5.1. АРМ, используемые для работы с государственными и муниципальными информационными системами (далее – ГИС и МИС) должны соответствовать требованиям,изложенным в документации соответствующих ГИС и МИС.

5.2. Перед началом работы в ГИС и МИС пользователи должны ознакомиться с правилами работы в соответствующих ГИС и МИС (инструкциями пользователям).

6. Правила работы в автоматизированной информационной системе документооборота и делопроизводства в Администрации Губернатора Самарской области, секретариате Правительства Самарскойобласти и органах исполнительной власти Самарской области

Работа в автоматизированной информационной системе документооборота и делопроизводства (далее – АИС ДД) Администрации Губернатора Самарской области, секретариате Правительства Самарской области и органах исполнительной власти Самарской области осуществляется с применением электронной подписи, в соответствии с приложением № 1 «Инструкции по делопроизводству в Администрации Губернатора Самарской области, секретариате Правительства Самарской области и органах исполнительной власти Самарской области», утвержденной распоряжением Губернатора Самарской области от 29.04.2013 № 234-р.

7. Правила антивирусной защиты

7.1. Для обеспечения антивирусной защиты должно использоваться сертифицированное лицензионное антивирусное программное обеспечение.

7.2. Ярлык антивирусной программы, как правило, находится в области уведомления или на вкладке «отображать скрытые значки» (нижний правый угол экрана).

7.3. Пользователи при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

7.4. Обновление антивирусной программы, как правило, производится автоматически, в противном случае необходимо обратиться к администратору ЛВС.

7.5. 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.

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

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

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

7.9. 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 в своем структурном подразделении;

– обратиться к инженеру обслуживающим Вашу вычислительную технику;

– обратиться в службу технической поддержки, установленной у Вас антивирусной программы и совместно с ними попытаться восстановить утраченную информацию.

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)!

8. Парольная политика

8.1. 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.

8.2. Полная плановая смена паролей пользователей должна проводиться регулярно (нереже 1 раза в 3 месяца).

8.3. 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.

8.4. В случае компрометации (утраты, разглашения, кражи, взлома) личного пароля пользователь должен немедленно предпринять меры по смене пароля.

8.5. Хранение пользователем значений своих паролей на материальном носителе допускается только в личном, запираемом ящике (сейфе).

8.6. 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.).

8.7. Правила формирования пароля:

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

8.7.2. В пароле должны присутствовать символы трех категорий из числа следующихчетырех:
– 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: !,$,#, %).

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

8.7.4. 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 рождениясвои и своих родственников, клички домашних животных, номера автомобилей, телефонови другие пароли, которые могут быть подобраны, основываясь на информации о пользователе.

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

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

8.7.7. Не использовать ранее использованные пароли.

8.7.8. При смене пароля новое значение должно отличаться от предыдущего не менеечем в 4 позициях.

8.7.9. Во время ввода пароля необходимо убедиться, что клавиатура находится вне поля зрения посторонних лиц, а также технических средств (видеокамер, фотоаппаратов).

8.7.10. Не использовать один пароль в разных информационных ресурсах.

9. Ответственность Пользователя

Пользователи несут персональную ответственность за свои действия в период осуществления информационного взаимодействия с использованием АРМ, за нарушение настоящего Свода правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, 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.