Приложение № 1
к приказу ГАПОУ МИК
от «___»_____20___ года №_____

УТВЕРЖДАЮ
Директор ГАПОУ МИК
И.В.Горшкова
«___»_____2021г.

Положение
об использовании сети Интернет
в ГАПОУ МИК

I. Общие положения

1. Настоящее Положение разработано во исполнение федерального закона № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», с учетом ГОСТ Р ИСО/МЭК 27002-2012 «Практические правила управления информационной безопасностью» и устанавливает порядок использовании сети Интернет в ГАПОУ МИК (далее образовательное учреждение).

2. Настоящее положение разработано в целях повышения уровня информационной безопасности и эффективности работы сотрудников образовательного учреждения.

3. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в образовательном учреждении.

4. Требования настоящего Положения распространяются на всех сотрудников образовательного учреждения и должны применяться для всех объектов информатизации, эксплуатируемых в образовательном учреждении.

5. Администратор узла и Администратор информационной безопасности назначаются приказом. Права и обязанности ответственных сотрудников описаны в разделе IV Настоящего положения.

II. Основные термины, сокращения и определения

Администратор узла – сотрудник (структурное подразделение) органа исполнительной власти, органа местного самоуправления муниципального образования и подведомственных им учреждений Оренбургской области, назначенный ответственным за настройку, обслуживание локальной вычислительной сети, ОИ и АРМ. Администратор узла является ответственным за подключение к сети Интернет.

Администратор информационной безопасности – сотрудник (структурное подразделение) органа исполнительной власти, органа местного самоуправления муниципального образования и подведомственных им

учреждений Оренбургской области, назначенный ответственным за информационную безопасность ОИ и АРМ в обслуживаемой локальной вычислительной сети.

Адрес IP – уникальный сетевой адрес объекта информатизации в сети, построенной на основе стека протоколов TCP/IP.

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.

«белый» ip-адрес – ip-адрес, не принадлежащий диапазону частных адресов и доступный из сети Интернет.

ЕИТКС – единая информационно-телекоммуникационная сеть Правительства Оренбургской области, утверждена постановлением Правительства Оренбургской области от 09.02.2017 № 94-п «Об утверждении положения о единой информационно-телекоммуникационной сети Правительства Оренбургской области».

Интернет – компьютерная сеть, представляющая собой глобальную систему соединенных компьютерных сетей, использующих стек протоколов TCP/IP для передачи/обмена данными.

ОИ – объект информатизации, являющийся компонентом ЕИТКС. В данное понятие входят серверы, компьютеры, планшеты, смартфоны, т.п.

ПО – программное обеспечение.

Пользователь – сотрудник образовательного учреждения, использующий ресурсы Интернет для выполнения своих должностных обязанностей.

Прокси-сервер – промежуточный сервер (комплекс программ), выполняющий роль посредника между пользователем и целевым сервером, позволяющий клиентам как выполнять косвенные запросы к другим сетевым службам, так и получать ответы.

САВЗ – средство антивирусной защиты

Интернет – компьютерная сеть, представляющая собой глобальную систему соединенных компьютерных сетей, использующих стек протоколов TCP/IP для передачи/обмена данными.

NAT – (англ. Network Address Translation – «преобразование сетевых адресов») – это механизм, позволяющий изменять IP-адрес в заголовке сетевого пакета, проходящего через устройство маршрутизации трафика.

VPN (англ. Virtual Private Network «виртуальная частная сеть») – территориально распределенная корпоративная логическая сеть, создаваемая на базе уже существующих сетей (локальных корпоративных сетевых структур, сетей связи общего пользования, сети Интернет, сетей связи операторов связи), имеющая сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных.

VPN-сервер – узел для построения логической сети.

III. Порядок подключения ОИ к сети Интернет

6. Для подключения ОИ к сети Интернет сотрудник образовательного учреждения, использующий данный ОИ, должен обратиться к Администратору узла.

7. Администратор узла организует настройку операционной системы на ОИ и ПО для доступа в Интернет.

8. ОИ может быть подключен к сети интернет по одному из трех способов:

а) стандартное подключение к сети Интернет;

б) подключение к сети Интернет с повышенной безопасностью;

в) прямое подключение к сети Интернет.

9. Стандартное подключение к сети Интернет осуществляется через прокси-сервер. Выбор используемого прокси-сервера выполняет Администратор узла. Адрес прокси-сервера указывается в настройках операционной системы или назначается контроллером домена.

10. Подключение к сети Интернет с повышенной безопасностью осуществляется через прокси-сервер. Выбор используемого прокси-сервера выполняет Администратор узла. Адрес прокси-сервера не указывается в настройках операционной системы и не назначается контроллером домена. Адрес прокси-сервера указывается в настройках непосредственно того ПО, которому необходимо обеспечить доступ к сети Интернет.

11. Прямое подключение к сети Интернет осуществляется с назначением ОИ «белого» ip-адреса или с применением технологии преобразования сетевых адресов (NAT).

а) серверы и маршрутизаторы. Данное подключение может использоваться только с разрешения Администратора информационной безопасности в образовательном учреждении (в таких случаях на схеме интеграции сервера/сервиса присутствует подпись Администратора информационной безопасности). Для данного способа подключения может использоваться только маршрутизирующее оборудование сегмента/узла ЕИТКС, имеющее действующий сертификат ФСТЭК России на соответствие требованиям документов «Требования к межсетевым экранам» и «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ».

б) АРМ (ОИ, подключенный к сегменту/узлу ЕИТКС). Допускается кратковременное использование данного типа подключения для АРМ только через VPN-сервер сегмента/узла ЕИТКС, который изолирует доступ к ресурсам ЕИТКС на время сетевой сессии.

Данное подключение осуществляется только с разрешения Администратора информационной безопасности в образовательном учреждении. Действия по данному подключению организуются Администратором информационной безопасности в образовательном учреждении. Для данного способа подключения может использоваться только VPN-сервер с применяемым средством защиты информации, сертифицированным ФСТЭК России на соответствие требованиям документов «Требования к системам обнаружения вторжений» и «Профиль защиты систем обнаружения вторжения уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ». Ответственность за конфиденциальность пароля учетной записи от VPN-сервера персональная для каждого сотрудника образовательного учреждения.

в) мобильные ОИ (не подключенные к сегменту/узлу ЕИТКС). Данное подключение не должно использовать сеть сегмента/узла ЕИТКС. Данный тип подключения может использовать оборудование операторов мобильной связи, доверенные Wi-Fi сети. Не допускается использование публичных Wi-Fi сетей с доступом без авторизации и Wi-Fi сетей, не входящих в перечень доверенных.

IV. Права и обязанности ответственных лиц

15. Администратор узла обязан:

а) производить настройку ОС для работы с прокси-сервером;

б) производить настройку ПО для работы с прокси-сервером;

в) производить настройку VPN подключений;

г) знать актуальную информацию о работе серверов (прокси, VPN).

16. Администратор узла имеет право:

а) получать от операторов серверов (прокси, VPN) разъяснения об их работе;

б) получать доступ к любому ОИ образовательного учреждения для выполнения своих обязанностей.

17. Администратор информационной безопасности обязан:

а) разрабатывать и согласовывать требования по подключению к сети Интернет ОИ образовательного учреждения;

б) контролировать выполнение требований настоящего Положения на ОИ образовательного учреждения;

в) оформлять инцидент информационной безопасности при поступлении информации об обнаружении неправомерного доступа в сеть Интернет ОИ образовательного учреждения.

18. Администратор информационной безопасности имеет право:

а) получать от операторов серверов (прокси, VPN) разъяснения об их работе;

б) получать доступ к любому ОИ образовательного учреждения для выполнения своих обязанностей.

V. Порядок использования сети Интернет

19. Доступ в сеть Интернет осуществляется централизованно с применением программных и программно-технических средств защиты (межсетевых экранов).

20. На ОИ, подключенному к сети Интернет, в обязательном порядке устанавливается САВЗ, которое эксплуатируется в соответствии с положением по антивирусной защите.

21. Использование сети Интернет допускается только при выполнении требований положения об антивирусной защите.

22. Запрещается использовать прямое подключение к сети Интернет, если для выполнения должностных обязанностей и задач достаточно подключения к сети Интернет с повышенной безопасностью или стандартного.

23. При использовании сети Интернет необходимо:

а) соблюдать требования настоящего Положения;

б) использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;

в) информировать Администратора информационной безопасности образовательного учреждения о любых фактах нарушения требований настоящего Положения.

Перечень типовых угроз при использовании сети Интернет и рекомендации по их предотвращению приведены в Приложении № 1 к Положению.

Общие меры предосторожности при использовании сети Интернет приведены в Приложении № 2 к Положению.

24. При использовании сети Интернет запрещено:

а) использовать предоставленный образовательным учреждением доступ к сети интернет в личных целях;

б) использовать специализированные аппаратные и программные средства, позволяющие сотрудникам образовательного учреждения получить несанкционированный доступ к сети Интернет;

в) публиковать, загружать и распространять материалы содержащие:

конфиденциальную информацию, а также информацию, составляющую персональные данные, за исключением случаев, когда это входит в служебные обязанности и способ передачи является допускает использование сети Интернет;

информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;

вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;

угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.;

г) фальсифицировать IP-адрес используемого ОИ, а также прочую служебную информацию;

д) устанавливать на ОИ ПО не соответствующее требованиям п. 24;

е) осуществлять попытки несанкционированного доступа к ресурсам сети Интернет, проведение сетевых атак и сетевого взлома, участие в них, за исключением случаев, если данные действия входят в полномочия сотрудника, проводятся в рамках анализа уязвимостей и согласованы с Администратором информационной безопасности в образовательном учреждении.

25. Разрешается устанавливать на ОИ только ПО, соответствующее условиям:

а) ПО является лицензионным. Лицензионное ПО может быть бесплатное (GNU General Public License – лицензия на свободное программное обеспечение);

б) источник ПО должен быть официальным и загружено только: с сайта разработчика; из официальных репозиториев операционных систем; из официальных магазинов приложений;

в) в лицензионном соглашении на ПО не должно быть условий передачи любых данных разработчику или третьим лицам, либо в ПО должна быть предусмотрена возможность отключения отправки любых данных разработчику или третьим лицам.

26. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО на прокси-сервере и САВЗ на ОИ пользователя.

27. Информация о посещаемых сотрудниками образовательного учреждения Интернет-ресурсах может протоколироваться для последующего анализа и, при необходимости, предоставляться руководителю образовательного учреждения.

28. Оператор прокси-сервера совместно с Администратором узла и Администратором информационной безопасности имеют право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, несущим угрозу информационной безопасности образовательного учреждения, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

29. В случае нарушения условий Положения Администратор информационной безопасности вправе, на время проведения проверки и анализа нарушения, отключить ОИ от доступа к сети Интернет, уведомив об этом руководителя образовательного учреждения и руководителя структурного подразделения, в котором произошло нарушение, либо вышестоящего должностного лица.

30. Расследование нарушений требований Положения производится в соответствии с положением о реагировании на инциденты информационной безопасности.

VI. Ответственность

31. Сотрудники образовательного учреждения, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами образовательного учреждения.

VII. Заключительные положения

32. Руководитель образовательного учреждения имеет право в целях обеспечения безопасности давать поручения о проведении администратором информационной безопасности проверок любого ОИ без предварительного уведомления сотрудников.

Приложение № 1
к Положению

Типовые угрозы
при работе с сетью Интернет

№ п/п	Угроза	Примечание	Рекомендуемые меры предосторожности
1.	Заражение компьютера вирусом	чаще всего, заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых»	установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
2.	Заражения компьютера вирусом при просмотре почтовых сообщений	обычно происходит при открытии прикрепленного к письму файла.	не открывать письма, если электронный адрес отправителя не знаком или выглядит «странно»; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
3.	Утечка информации с рабочей станции	уязвимым может оказаться программное обеспечение (чаще всего таковым является свободно распространяемое ПО, а также ПО от неизвестных или малоизвестных производителей). Также причиной утечки может оказаться заражение компьютера вирусом	использовать только лицензионное ПО; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
4.	Предоставление возможности	такая возможность может быть получена	использовать только лицензионное ПО;

	удаленного управления компьютером	как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом)	установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
5.	Потеря функциональности (полная или частичная) рабочей станции	чаще всего это происходит вследствие использования уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом	использовать только лицензионное ПО; установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
6.	Кража личной информации	чаще всего к этому приводит ввод такой информации на веб-страницах (фишинговые страницы), в том числе сайтах-двойниках, которые внешне идентичны настоящим сайтам (например, сайту банка), но на самом деле являются подделкой	не открывать письма (и особенно вложения) от незнакомых адресатов; внимательно проверять адрес страницы, на которой вы собираетесь оставить личную информацию; не сохранять пароли в формах веб-страниц и в браузере.
7.	Захват адресов электронной почты, веб-страниц и т.п.	чаще всего к этому приводит использование «слабого» пароля для доступа к ресурсу, а также подбор ответа на контрольной вопрос, используемый для восстановления пароля в случае его возможной утери	выполнять требования положения по парольной защите.

Приложение № 2
к Положению

Общие меры предосторожности
при работе с сетью Интернет

№ п/п	Мера предосторожности	Примечание
1.	Мониторинг обновлений ПО, используемого на ОИ образовательного учреждения, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.
2.	Приостановка эксплуатацию используемого ПО в случае обнаружения критических, с точки зрения безопасности, уязвимостей и невозможности их устранения.	Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на пользователей и администраторов соответствующих ОИ образовательного учреждения.
3.	При работе с электронной почтой: антивирусная проверка любых прикрепленных файлов перед их запуском или открытием; запрет на открытие писем с вложенными файлами от неизвестных авторов.	Одним из наиболее часто используемых каналов распространения вирусов, а также кражи личной информации, является электронная почта. В случае возникновения вопросов по вложенным файлам во входящих сообщениях электронной почты необходимо обратиться к администратору информационной безопасности до принятия решения о дальнейших действиях. Ответственность возлагается на Пользователей.
4.	Запрет автоматического сохранения и/или запуска файлов и элементов ActiveX, скриптов из сети Интернет на рабочей станции пользователя.	Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или

		через сами веб-страницы, которые содержат вредоносный/опасный код. Для опытных пользователей с разрешения отдела по защите информации допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов. Ответственность возлагается на Пользователей.
5.	Запрет на сохранение паролей в заполняемых формах при посещении веб-страниц.	Сохранение пароля может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на Пользователей.