

ГБОУ средняя общеобразовательная школа № 51  
Петроградского района  
Санкт-Петербурга

Государственное бюджетное общеобразовательное учреждение  
средняя общеобразовательная школа № 51 Петроградского района Санкт-Петербурга

31.08.2024 12:08  
директор  
197110, СПб, Чкаловский пр. д. 22, лит. А  
Березяк Элина Арвовна  
7813124534-5-1724061729-20240819-231-1-1302-09

тел/ф (812) 417-62-12

## П Р И К А З

31 августа 2024г.

№ 259

Об использовании сети Интернет  
и электронной почты

В соответствии с Федеральным законом Российской Федерации от 27.07.2006г. №149-ФЗ "Об информации, информационных технологиях и о защите информации"  
**ПРИКАЗЫВАЮ:**

1. Утвердить Положение об использовании сети Интернет и электронной почты Государственного бюджетного образовательного учреждения средняя общеобразовательная школа №51 Петроградского района Санкт-Петербурга (согласно Приложению № 1 к приказу).
2. Утвердить Перечень типичных угроз при работе с сетью Интернет и электронной почтой Государственного бюджетного образовательного учреждения средняя общеобразовательная школа № 51 Петроградского района Санкт-Петербурга (согласно Приложению № 2 к приказу).
3. Утвердить Общие меры предосторожности при работе с сетью Интернет и электронной почтой Государственного бюджетного образовательного учреждения средняя общеобразовательная школа № 51 Петроградского района Санкт-Петербурга (согласно Приложению № 3 к приказу).
4. Контроль за исполнением приказа оставляю за собой.

Директор

Э.А. Березяк

ГБОУ средняя общеобразовательная школа № 51  
Петроградского района  
Санкт-Петербурга

Подписано электронной подписью

31.08.2024 12:08

директор

Березяк Элина Арвовна

7813124534-5-1724061759-20240819-231-1-1302-39

Государственное бюджетное общеобразовательное учреждение

средняя общеобразовательная школа № 51 Петроградского района Санкт-Петербурга

197110, СПб, Каловский пр. д. 22, лит. А

тел/ф (812) 417-62-12

**УТВЕРЖДАЮ**

Директор ГБОУ СОШ № 51

Петроградского района СПб

Приказ от 31 августа 2024г. №259

\_\_\_\_\_ Э.А. Березяк

**ПРИНЯТО**

Совет Образовательного учреждения

ГБОУ СОШ № 51

Петроградского района СПб

Протокол от 30 августа 2024г. №1

**СОГЛАСОВАНО**

Профсоюзный комитет

ГБОУ СОШ №51 Петроградского района СПб

Протокол от 30 августа 2024г. №1

\_\_\_\_\_ Е.А.Горбачева

## Положение

### об использовании сети интернет и электронной почты

### Государственного бюджетного образовательного учреждения средняя общеобразовательная школа № 51 Петроградского района Санкт-Петербурга

#### 1. Общие положения

1.1. Настоящее Положение разработано во исполнение Концепции информационной безопасности Государственного бюджетного образовательного учреждения средняя общеобразовательная школа № 51 Петроградского района Санкт-Петербурга (далее – ГБОУ) в соответствии с Федеральным законом № 149-ФЗ от 26.07.2006 г. «Об информации, информационных технологиях и о защите информации» (ред. 18.03.2019), ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» (27002-2012 ред. 24.09.2012 № 423-ст) и другими нормативными правовыми актами, и устанавливает порядок использования сети Интернет и электронной почты работниками ГБОУ.

1.2. Действие настоящего Положения распространяется на работников ГБОУ, подключенных к сети Интернет, подрядчиков и третью сторону.

#### 2. Основные термины, сокращения и определения

**Адрес IP** – уникальный идентификатор АРМ, подключенного к ИС ГБОУ, а также сети Интернет.

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

**Интернет** – глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.

**АС** – автоматизированная система ГБОУ – система, обеспечивающая хранение, обработку, преобразование и передачу информации ГБОУ с использованием компьютерной и другой техники.

**ИТ** – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации ГБОУ с использованием средств компьютерной и другой техники.

**Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

**ПК** – персональный компьютер.

**ПО** – программное обеспечение вычислительной техники, базы данных.

**ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

**ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

**Пользователь** – работник ГБОУ, использующий ресурсы Интернет для выполнения своих должностных обязанностей.

**Реестр** – документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в ГБОУ.

**Электронная почта** – сервис обмена электронными сообщениями в рамках АС ГБОУ (внутренняя электронная почта) и общедоступных сетей Интернет (внешняя электронная почта).

**Электронное почтовое сообщение** – сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.

**Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.

**Электронный почтовый ящик** – персональное пространство на почтовом сервере, в котором хранятся электронные сообщения.

### **3. Порядок использования сети Интернет и электронной почты**

3.1. Доступ в сеть Интернет и к электронной почте (далее – к Сервисам) в ГБОУ осуществляется централизованно с применением специальных программно-технических средств защиты (межсетевых экранов).

3.2. Доступ к Сервисам с использованием мобильных устройств (мобильного Интернета) допускается только в удаленных подразделениях (филиалах) ГБОУ. Все мобильные устройства должны быть учтены в журнале учета съемных носителей и устройств передачи данных ГБОУ.

3.3. На АРМ, подключенное к сети Интернет, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.

3.4. Доступ к Сервисам предоставляется ограниченному кругу Пользователей в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам, для обмена служебной информацией в виде электронных сообщений и документов в электронном виде в интересах ГБОУ после ознакомления с настоящим Положением и Приложениями к нему.

3.5. Для доступа работников ГБОУ к Сервисам допускается применение коммерческого или бесплатного ПО, входящего в Реестр разрешенного к использованию ПО и указанного в Паспорте ПК.

3.6. Доступ работнику ГБОУ к Сервисам может быть инициирован Руководством ГБОУ:

- необходимости организации АРМ для нового работника;

- необходимости выполнения работником новых (дополнительных) обязанностей, для которых требуется доступ к внешним ресурсам.
- 3.7. Операции по предоставлению доступа работников ГБОУ к Сервисам и их техническому обеспечению выполняются в соответствии с «Порядком доступа к информационным, программным и аппаратным ресурсам ГБОУ» Руководством ГБОУ через заявки на имя Руководителя ГБОУ, подписанные сотрудником и согласованные с Руководством ГБОУ.
- 3.8. При использовании Сервисов необходимо:
- 3.8.1. Соблюдать требования настоящего Положения.
- 3.8.2. Использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.
- 3.8.3. Ставить в известность отдел по защите информации о любых фактах нарушения требований настоящего Положения.
- 3.8.4. Типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в Приложении №1.
- 3.8.5. Общие меры предосторожности при работе с Сервисами приведены в Приложении №2.
- 3.9. При использовании Сервисов запрещено:
- 3.9.1. Использовать предоставленный ГБОУ доступ к Сервисам в личных целях.
- 3.9.2. Использовать специализированные аппаратные и программные средства, позволяющие работникам ГБОУ получить несанкционированный доступ к Сервисам.
- 3.9.3. Публиковать, загружать и распространять материалы содержащие:
- конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, персональные данные, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом по защите информации заранее;
  - 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.
- 3.9.4. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.
- 3.9.5. Распространять и устанавливать на других ПЭВМ любое программное обеспечение и данные, полученные с использованием Сервисов.
- 3.9.6. Осуществлять попытки несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них.
- 3.9.7. Переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей.
- 3.9.8. По собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений, если рассылка не связана с выполнением служебных обязанностей.
- 3.9.10. Использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей.

- 3.9.11. Публиковать свой электронный адрес, либо электронный адрес других работников Организации на общедоступных Интернет-ресурсах (форумы, конференции и т.п.).
- 3.9.12. Предоставлять работникам ГБОУ (за исключением Руководства ГБОУ) и третьим лицам доступ к своему электронному почтовому ящику.
- 3.9.13. Перенаправлять электронные сообщения с личных почтовых ящиков на корпоративный.
- 3.9.14. Запрещается использование в качестве паролей для доступа к ресурсам Сервисов паролей, аналогичных паролям, используемым для доступа к ресурсам ГБОУ.
- 3.9.15. Запрещается отключать установленное на АРМ антивирусное программное обеспечение.
- 3.10. Содержание Интернет-ресурсов, а также файлы, загружаемые из Сервисов, подлежат обязательной проверке на отсутствие вредоносного ПО.
- 3.12. Информация о посещаемых работниками ГБОУ Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть предоставлена Руководству ГБОУ для контроля.
- 3.13. Руководство ГБОУ оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.
- 3.14. ГБОУ оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего Положения.
- 3.15. В случае нарушения пунктов Положения Руководство ГБОУ вправе отключить АРМ от Сервисов, уведомив об этом руководство структурного подразделения.
- 3.16. Расследование допущенных нарушений Положения производится на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в ГБОУ.

#### **4. Ответственность**

- 4.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами ГБОУ.

#### **5. Заключительные положения**

- 5.1. Анализ актуальности данного Положения должен проводиться Руководством ГБОУ не реже одного раза в год, а также в каждом случае внедрения новых сервисов в дополнение к имеющимся. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Положение, новая редакция Положения должна быть утверждена приказом по ГБОУ.
- 5.2. Контроль над соблюдением требований данного Положения проводится Руководством ГБОУ.

ГБОУ средняя общеобразовательная школа № 51  
Петроградского района  
Санкт-Петербурга

Подписано электронной подписью  
31.08.2024 12:08

директор

Березяк Элина Арвовна

7813124534-5-1724061801-20240819-231-1-1303-21

УТВЕРЖДЕНО

Приказ от 31 августа 2024г. №259

Директор \_\_\_\_\_ Э.А.Березяк

## ТИПИЧНЫЕ УГРОЗЫ ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТОЙ

№ 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».	- не посещать перечисленные сайты; - 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 вам не знаком или выглядит «странно»; - не открывать прикрепленные файлы, если отправитель письма вам неизвестен; - 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 принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
4.	Предоставление возможности удаленного управления компьютером.	Такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом).	- использовать только принятое к использованию в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
5.	Потеря функциональности (полной или частичной)	Чаще всего это происходит вследствие использования	- использовать только принятое к использованию

	рабочей станцией.	уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом.	в Организации программное обеспечение; - установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
6.	Кража личной информации.	Чаще всего к этому приводит ввод такой информации на веб-страницах, 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.
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.	- использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр); - не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию; - никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям; - не сохранять пароли в формах веб-страниц.

**ТИПИЧНЫЕ УГРОЗЫ  
ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТОЙ**

№ п/п	Угроза	Примечание	Рекомендуемые меры предосторожности
8.	Заражение компьютера вирусом.	Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых».	<ul style="list-style-type: none"> <li>- не посещать перечисленные сайты;</li> <li>- установить, своевременно обновлять и не отключать антивирусное программное обеспечение.</li> </ul>
9.	Заражения компьютера вирусом при просмотре почтовых сообщений.	Обычно происходит при открытии прикрепленного к письму файла.	<ul style="list-style-type: none"> <li>- не открывать письма, если электронный адрес отправителя вам не знаком или выглядит «странно»;</li> <li>- не открывать прикрепленные файлы, если отправитель письма вам неизвестен;</li> <li>- установить, своевременно обновлять и не отключать антивирусное программное обеспечение.</li> </ul>
10.	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.	<ul style="list-style-type: none"> <li>- использовать только принятое к использованию в Организации программное обеспечение;</li> <li>- установить, своевременно обновлять и не отключать антивирусное программное обеспечение.</li> </ul>
11.	Предоставление возможности удаленного управления компьютером.	Такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом).	<ul style="list-style-type: none"> <li>- использовать только принятое к использованию в Организации программное обеспечение;</li> <li>- установить, своевременно обновлять и не отключать антивирусное программное обеспечение.</li> </ul>
12.	Потеря функциональности (полной или частичной) рабочей станцией.	Чаще всего это происходит вследствие использования уязвимостей программного обеспечения	<ul style="list-style-type: none"> <li>- использовать только принятое к использованию в Организации программное обеспечение;</li> </ul>

		злоумышленником или из-за заражения вирусом.	- установить, своевременно обновлять и не отключать антивирусное программное обеспечение.
13.	Кража личной информации.	Чаще всего к этому приводит ввод такой информации на веб-страницах, 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.
14.	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.	- использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр); - не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию; - никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям; - не сохранять пароли в формах веб-страниц.

ГБОУ средняя общеобразовательная школа № 51  
Петроградского района  
Санкт-Петербурга

Подписано электронной подписью  
31.08.2024 12:08

директор

Березяк Элина Арвовна

7813124534-5-1724061870-20240819-231-1-1304-30

УТВЕРЖДЕНО

Приказ от 31 августа 2024г. №259

Директор \_\_\_\_\_ Э.А.Березяк

## ОБЩИЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТОЙ

№ п/ п	Мера предосторожности	Примечание
1.	Использование только разрешенного отделом информационных технологий и отделом по защите информации программного обеспечения.	Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО. Ответственность возлагается на пользователя.
2.	Отслеживание появления обновлений ПО, используемого на компонентах АС Организации, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на администраторов соответствующих компонентов.
3.	В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО.	Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на пользователей и администраторов соответствующих компонентов АС Организации.
4.	Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС Организации, взаимодействующих с сетью Интернет, в режиме мониторинга событий.	Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет. Ответственность возлагается на администраторов соответствующих компонентов.
5.	При работе с электронной почтой – не открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку.	В последнее время наиболее распространенный канал распространения вирусов, а также кражи личной информации – электронная почта. В случае возникновения вопросов

		необходимо обратиться в отдел по защите информации до принятия решения о дальнейших действиях. Ответственность возлагается на пользователей.
6.	Запретить автоматическое сохранение и/или запуск 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.
7.	Не рекомендуется сохранять пароли в формах при посещении веб-страниц.	Это может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем. Ответственность возлагается на пользователей.

**ОБЩИЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ  
ПРИ РАБОТЕ С СЕТЬЮ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТОЙ**

№ п/ п	Мера предосторожности	Примечание
8.	Использование только разрешенного отделом информационных технологий и отделом по защите информации программного обеспечения.	Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО. Ответственность возлагается на пользователя.
9.	Отслеживание появления обновлений ПО, используемого на компонентах АС Организации, взаимодействующих с сетью Интернет.	ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на администраторов соответствующих компонентов.
10.	В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО.	Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя. Ответственность возлагается на пользователей и администраторов соответствующих компонентов АС Организации.
11.	Обязательное использование и своевременное обновление антивирусного ПО на компонентах АС Организации, взаимодействующих с сетью Интернет, в режиме мониторинга событий.	Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет. Ответственность возлагается на администраторов соответствующих компонентов.
12.	При работе с электронной почтой – не открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку.	В последнее время наиболее распространенный канал распространения вирусов, а также кражи личной информации – электронная почта. В случае возникновения вопросов необходимо обратиться в отдел по защите информации до принятия решения о дальнейших действиях.

		Ответственность возлагается на пользователей.
13.	Запретить автоматическое сохранение и/или запуск файлов и элементов ActiveX, скриптов из сети Интернет на рабочей станции пользователя.	<p>Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или через сами веб-страницы, которые содержат вредоносный/опасный код.</p> <p>Для опытных пользователей с разрешения отдела по защите информации допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов.</p> <p>Ответственность возлагается на пользователей.</p>
14.	Не рекомендуется сохранять пароли в формах при посещении веб-страниц.	<p>Это может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем.</p> <p>Ответственность возлагается на пользователей.</p>





