

УСЛОВИЯ

информационного взаимодействия при тестировании специального программного обеспечения, с помощью которого осуществляется дистанционное электронное голосование

1. Общие положения

1.1. На стоящие Условия информационного взаимодействия при тестировании на уязвимости специального программного обеспечения MOS.RU, с использованием которого осуществляется дистанционное электронное голосование (далее – Условия), содержат существенные условия соглашения об участии заинтересованных лиц в тестировании на уязвимости информационной системы, с использованием которой осуществляется дистанционное электронное голосование, для обеспечения информационной безопасности при проведении дистанционного электронного голосования в городе Москве на выборах депутатов Московской городской Думы седьмого созыва в соответствии с Федеральным законом от 29.05.2019 N 103-ФЗ «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» и Законом города Москвы от 22.05.2019 N 18 «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва».

1.2. Настоящие Условия должны быть приняты заинтересованными лицами в полном объеме, без оговорок, изъятий и ограничений, способом, указанным в разделе 2 настоящих Условий.

1.3. В настоящих Условиях используются следующие основные понятия:

1.3.1. Организатор – Департамент информационных технологий города Москвы.

1.3.2. Участник – физическое лицо, индивидуальный предприниматель, организация, принявшие настоящие Условия и получившие уведомление о возможности участия в тестировании.

1.3.3. Система – специальное программное обеспечение MOS.RU, с использованием которого осуществляется дистанционное электронное голосование в городе Москве на выборах депутатов Московской городской Думы седьмого созыва.

1.3.4. Уязвимости – недостатки Системы, которые могут быть использованы для реализации угроз безопасности информации.

1.3.5. Тестирование – моделирование действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации Системы.

1.4. Тестирование осуществляется в период с 16 июля по 1 августа 2019 года. Прием заявлений осуществляется с момента публикации указанного Соглашения.

1.5. Информационное взаимодействие осуществляется на безвозмездной основе.

2. Порядок заключения Соглашения

2.1. В целях заключения Соглашения заинтересованные лица принимают настоящие Условия путем подачи Организатору заявления по форме согласно приложению к настоящим Условиям.

2.2. Организатор сторона обязуется заключить Соглашение с любым лицом, подавшим заявление о принятии настоящих Условий, при соблюдении следующих требований:

2.2.1. Предоставление полных, достоверных и актуальных сведений о заявителе на электронный адрес support-vybory@mos.ru

2.2.2. Указание программных средств, которые будут использоваться заявителем для тестирования.

2.2.3. Обязательство Заявителя выполнять настоящие Условия в полном объеме.

2.3. Заявление подается в электронной форме физическим лицом, индивидуальным предпринимателем, руководителем юридического лица или уполномоченным представителем, действующим на основании доверенности. Заявление организации заверяется печатью организации и направляется в виде сканированной копии. В случае подписания представителем по доверенности к заявлению прилагается сканированная заверенная копия доверенности. Заявление также может быть подано в форме электронного документа, подписанного электронной подписью.

2.4. Организатор при получении заявления проверяет указанные в заявлении сведения и при соблюдении требований, указанных в п.2.2 настоящих Условий, направляет заявителю уведомление о возможности участия в тестировании и сетевые адреса стендов для тестирования с использованием контактной информации, указанной в заявлении, в форме электронного документа.

2.5. Основаниями для отклонения заявления являются:

2.5.1. Неполнота, недостоверность или неактуальность сведений, указанных в заявлении.

2.5.2. Неуказание программных средств или IP адресов, которые будут использоваться заявителем для тестирования.

2.6. При наличии оснований для отклонения заявления Организатор направляет заявителю уведомление о невозможности участия в тестировании с указанием причин невозможности с использованием контактной информации, указанной в заявлении, в форме электронного документа.

3. Права и обязанности Сторон

3.1. Организатор:

3.1.1. Направляет участникам сценарии и сетевые адреса стендов для тестирования.

3.1.2. Обеспечивает работоспособность стендов для тестирования в период тестирования.

3.1.3. Анализирует результаты тестирования и учитывает их при выполнении работ по обеспечению безопасности информации Системы.

3.2. Участник:

3.2.1. Обеспечивает использование при тестировании программного обеспечения, указанного в заявлении.

4. Техническая организация тестирования

4.1. Тестирование осуществляется на стендах – компонентах Системы (далее – стенды), включающих совокупность информации и обеспечивающих ее обработку информационных технологий и технических средств. Конфигурация компонентов позволяет выявлять и анализировать в ходе тестирования уязвимости различных видов. Состав информации специально подобран для тестирования с учетом возможности нарушения ее безопасности.

4.2. Доступ к стендам организуется с использованием сети Интернет. Доступ к стендам осуществляется с IP адресов, указанных участником взаимодействия в заявлении. Реквизиты доступа к стендам направляются на электронную почту участника взаимодействия.

4.3. Основные направления тестирования:

Направления тестирования	Цель тестирования
Организация Ddos-атаки на весь портал mos.ru	Невозможно проголосовать, сайт не работает целиком
Организация Ddos-атаки на систему авторизации СУДИР	Невозможно проголосовать, не работает аутентификация
Организация Ddos-атаки на Единый личный кабинет	Невозможно проголосовать, не работает подтверждение личности
Организация Ddos-атаки на инфраструктуру	Невозможно проголосовать
Подбор пары-логин и пароль, несанкционированное получение доступа к Личному кабинету	Получение доступа к чужому кабинету, если человек использовал одинаковую почту и пароль на других сайтах, где произошла утечка. Потенциальная возможность проголосовать не за себя.
Нахождение и использование уязвимостей интерактивных форм МПГУ и СУДИР с целью остановки работы	Невозможно проголосовать, нарушена работа функционала.
Нахождение и использование уязвимостей интерактивных форм МПГУ и СУДИР с целью проголосовать дважды, порчи бюллетеня и т.д.	Мошеннические действия, искажение результатов голосования.
Нахождение уязвимости Блокчейн для записи некорректной информации	Мошеннические действия, искажение результатов голосования.
Внутренний нарушитель, администратор	Мошеннические действия, искажение результатов голосования.

4.4. Основные сценарии тестирования:

Сценарий 1.

Не обладающий активным избирательным правом гражданин должен обойти проверки и попасть на форму предзаписи. Задача: попасть на форму и отправить заявление на включение в списки.

Стенд:

https://newmos.mos.ru/pgu/ru/app/index.php?org_id=mgik&form_id=mgd2019

Сценарий 2.

Гражданин обладает активным избирательным правом, все проверки пройдены, эмулируем генерацию лишних избирателей в реестре избирателей.

Код базовой авторизации будет отправлен в ответ на заявку.

Задача: попробовать через форму записать множество граждан, либо сделать форму недоступной для любого гражданина.

Стенд:

<https://newmos.mos.ru/pgu/ru/app/studsovet/vybory-golosovanie/>

Сценарий 3.

Гражданин не включен в реестр избирателей.

Задача: получить доступ к бюллетеню в обход проверки по реестру избирателей.

Стенд:

<https://newmos.mos.ru/pgu/ru/app/mgik/mgd-golosovanie/>

Сценарий 4.

Гражданин получил доступ к форме голосования после всех проверок по реестру избирателей.

Задача: даем неограниченное количество попыток голосования с целью, определяемыми самим тестирующим.

Стенд:

<https://newmos.mos.ru/pgu/ru/app/mgik/mgd-golosovanie/>

Ключ доступа добавим в ответ на заявку.

Сценарий 5.

Организатор не реже одного раза в сутки размещает на <https://github.com/moscow-technologies/> открытый ключ шифрования и набор данных, зашифрованный открытым ключом алгоритмами, используемыми для шифрования голоса избирателя в голосовании. Каждые 12 часов (продолжительность голосования) публиковаться соответствующий закрытый ключ, которым можно расшифровать эти данные. Задача, стоящая перед техническими специалистами, сводится к попытке расшифровать данные до момента появления соответствующего закрытого ключа.

4.4. Организатор организует перезапуск голосования один раз в сутки (сбрасывается счетчик голосования, таким образом учетная запись Портала mos.ru может быть использована для повторного голосования).

4.5. Для реализации сценариев тестирования не ограничивается использование любых учетных записей портала mos.ru

4.5.1. Для запроса базовой авторизации и доступа к стендам направляется заполненное Заявление о принятии условий на адрес support-vybory@mos.ru

Организатор в ответ направляет логин и пароль для доступа к стендам (базовая авторизация).

4.5.2. Для выполнения Сценария 4 данные учетные записи портала mos.ru, с которых планируется проводить тестирование должны быть направлены для включения в тестовый реестр на адрес support-vybory@mos.ru

4.5.3. Для выполнения других сценариев может быть использована любая учетная запись mos.ru прошедшая регистрацию в установленном порядке.

5. Правовые аспекты тестирования

5.1. Нарушение безопасности информации не повлечет причинения вреда правам и охраняемым законом интересам. Действия участников тестирования не образуют состава правонарушения в связи с предварительным согласием собственника информационных ресурсов и открытым характером действий в процессе тестирования.

6. Действие соглашения

6.1. Соглашение вступает в силу с даты получения участником уведомления о возможности участия в тестировании.

6.2. Организатор вправе в любой момент приостановить, прекратить тестирование без объяснения причин.

6.3. Организатор вправе в любое время вносить изменения в настоящие Условия. Новая редакция Условий доводится до участников тестирования в электронной форме и размещается на новостном ресурсе MOS.RU

Приложение к Условиям
информационного взаимодействия при
тестировании специального
программного обеспечения, с помощью
которого осуществляется дистанционное
электронное голосование
информационного

Заявление о принятии Условий

1. Заявитель:

Ф.И.О. физического лица, индивидуального предпринимателя

полное наименование юридического лица

сокращенное наименование юридического лица

дата регистрации юридического лица/индивидуального

предпринимателя

ОГРН/ОГРНИП

ИНН

Сведения о лице, действующем без доверенности от имени
юридического лица.

2. Заявитель подтверждает полное и безоговорочное принятие Условий
информационного взаимодействия при тестировании специального
программного обеспечения, с помощью которого осуществляется
дистанционное электронное голосование.

3. Для тестирования будут применяться следующие программные
средства:

4. Тестирование будет производиться со следующих IP адресов:

5. Контактная информация для направления уведомлений.

6. Прошу внести в список для голосования в рамках тестирования
следующие учетные записи портала mos.ru: (перечень СНИЛС, либо
телефон/email).