|  |  |  |
| --- | --- | --- |
| ОГРН 1155200000273 |  | УТВЕРЖДЕНООбщим собранием СТЭППротокол от 05 марта 2020 года |

**ПОЛОЖЕНИЕ**

**УСЛОВИЯ ЧЛЕНСТВА В СОЮЗЕ ТОРГОВЫХ ЭЛЕКТРОННЫХ ПЛОЩАДОК**

1. **Общие положения**
	1. Настоящее положение разработано в соответствии с Федеральными законами РФ «О несостоятельности (банкротстве)», «О Саморегулируемых организациях», «О Некоммерческих организациях», руководящим документом (РД) Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Приказом ФСТЭК России от 18.02.2013 № 21, Приказом Минэкономразвития РФ №495 от 23.07.2015г., Приказом ФСБ России от 10.07.2014 № 378, Приказом Гостехкомиссии России от 30.08.2002 № 282, Уставом и иными внутренними документами некоммерческой организации Союз Торговых Электронных Площадок (далее – «Союз» или «СТЭП») и определяет условия членства в Союзе.
	2. Настоящее положение в части типовых требований к информационной безопасности в информационной системе для проведения торгов в электронной форме разработано на основании Договора №16-09/01 от «01» сентября 2016 года с ООО «ЛИССИ-Софт», действующего на основании лицензии ФСТЭК России регистрационный № 1858 от «11» октября 2012 года на деятельность по технической защите конфиденциальной информации и лицензии ФСБ России регистрационный № 13172 Н от «27» сентября 2013 года на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.
	3. Настоящее положение устанавливает в соответствии с пунктами 14 и 20 статьи 110 Федерального закона «О несостоятельности (банкротстве)» от 26.10.2002 N 127-ФЗ требования к операторам электронных площадок, электронным площадкам, в том числе технологическим, программным, лингвистическим, правовым и организационным средствам, необходимым для проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве.
2. **Членство в Союзе.**
	1. Членство в Союзе могут приобретать исключительно субъекты предпринимательской деятельности (индивидуальные предприниматели и (или) юридические лица), которые осуществляют профессиональную деятельность по проведению торгов в электронной форме в качестве владельцев автоматизированных систем проведения торгов (Операторы электронных площадок).
	2. Принадлежность субъекта предпринимательской деятельности к профессиональной сфере деятельности Оператора электронной площадки определяется на основании кодов ОКВЭД, включённых в перечень видов деятельности такого субъекта:

63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов

62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая

47.91.2 Торговля розничная, осуществляемая непосредственно при помощи информационно-коммуникационной сети Интернет.

* 1. Операторы электронных площадок приобретают статус членов Союза с даты вступления в силу решения Общего собрания членов Союза о приеме субъекта предпринимательской, профессиональной деятельности в члены СТЭП.
	2. Членство оператора электронной площадки в Союзе прекращается по решению Общего собрания его членов (с даты, следующей за датой принятия такого решения) на основании заявления оператора электронной площадки о выходе из Союза или в случае исключения оператора электронной площадки из Союза в связи с нарушением им:

- условий членства в Союзе;

- требований Федерального закона «О несостоятельности (банкротстве)», других федеральных законов, иных нормативных правовых актов Российской Федерации, стандартов и правил профессиональной деятельности операторов электронных площадок.

Решение суда о прекращении функционирования лица в качестве оператора электронной площадки в отношении члена СТЭП также является основанием для прекращения членства.

Сведения о прекращении членства оператора электронной площадки включаются в реестр членов СТЭП.

1. **Условия членства в Союзе.**
	1. Требования к операторам электронных площадок (Операторам ЭП).
		1. В период членства в СТЭП оператор электронной площадки должен сохранять в установленном законом порядке государственную регистрацию на территории Российской Федерации, как юридическое лицо независимо от его организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала или физическое лицо в качестве индивидуального предпринимателя.
		2. В период членства в СТЭП не должно проводится ликвидации юридические лица и (или) индивидуального предпринимателя оператора электронной площадки.
		3. Решения арбитражного суда о введении процедуры в деле о несостоятельности (банкротстве) в соответствии с законодательством о банкротстве в отношении оператора электронной площадки – члена СТЭП не должно быть принято.
		4. Сведения об операторе электронной площадки – члене СТЭП должны отсутствовать в реестре недобросовестных поставщиков.
		5. В отношении оператора электронной площадки – члена СТЭП должно отсутствовать вступившее в законную силу решение арбитражного суда о прекращении функционирования лица в качестве оператора электронной площадки.
		6. Оператор электронной площадки должен иметь действующий договор обязательного страхования ответственности за причинение убытков третьим лицам при проведении торгов в электронной форме в связи с неисполнением или ненадлежащим исполнением оператором электронной площадки требований, установленных законодательством Российской Федерации, стандартами и правилами профессиональной деятельности операторов электронных площадок. Договор должен быть заключен со страховой организацией, аккредитованной саморегулируемой организацией операторов электронных площадок, на срок не менее чем один год с условием его возобновления на тот же срок. Минимальный размер страховой суммы по договору обязательного страхования ответственности оператора электронной площадки составляет тридцать миллионов рублей в год.
		7. Оператор электронной площадки обязан вносить взносы, в установленном Союзом размере и порядке, а также взносы в компенсационный фонд Союза.
		8. Оператор электронной площадки на законных основаниях должен обладать необходимыми правами на программные и технические средства, обеспечивающие функционирование электронной площадки для проведения торгов.
		9. Оператор электронной площадки должен владеть сайтом электронной площадки в информационно-телекоммуникационной сети "Интернет", электронный адрес которого включает доменное имя, права на которое принадлежат оператору электронной площадки.
		10. Оператор ЭП должен обеспечивать бесперебойное функционирование предназначенных для проведения торгов электронной площадки и программно-аппаратного комплекса, доступ к ним пользователей, в том числе заявителей, в течение всего срока проведения торгов.
		11. Оператор ЭП должен обеспечивать равный доступ всех лиц к участию в торгах, в том числе к информации о проведении торгов, без взимания с них платы.
		12. Оператор ЭП должен обеспечивать при проведении торгов техническую поддержку организаторов торгов, лиц, представивших заявки на участие в торгах, и участников торгов в режиме не менее пяти дней в неделю, не менее двенадцати часов подряд в течение одного рабочего дня при выделении для этих целей не менее трех телефонных линий и не менее трех операторов для ответа на телефонные звонки (время ожидания ответа не должно превышать пяти минут), а также не менее трех операторов для ответа на сообщения, полученные по электронной почте (служба технической поддержки).
		13. Оператор ЭП должен обеспечивать контроль за соответствием электронной площадки установленным к ней требованиям.
		14. Оператор ЭП должен обеспечивать непрерывность проведения торгов, функционирование программных и технических средств, используемых для проведения торгов, а также равный доступ участников торгов к участию в торгах.

В случае, если оператор электронной площадки осуществляет обработку сведений, в отношении которых требуется обеспечение их конфиденциальности в соответствии с законодательством Российской Федерации, оператор электронной площадки обязан иметь соответствующее разрешение (лицензию) на обработку указанных сведений.

* + 1. Оператор ЭП должен обеспечивать возможность представления заявки на участие в торгах и прилагаемых к ней документов, их копий в форме электронных документов.
		2. Оператор электронной площадки должен обеспечивать возможность заключения с заявителями на участие в торгах договоров о задатке.
		3. Оператор ЭП должен обеспечивать свободный и бесплатный доступ к информации о проведении торгов, правилах работы электронной площадки.
		4. Оператор ЭП должен обеспечивать свободный круглосуточный бесперебойный доступ к электронной площадке через информационно-телекоммуникационную сеть "Интернет" в течение всего времени проведения торгов организаторам торгов, заявителям на участие в торгах, а также участникам торгов в соответствии с правами, предоставленными указанным лицам согласно законодательству Российской Федерации, в том числе согласно порядку проведения торгов.
		5. Оператор ЭП должен обеспечивать хранение и обработку в электронной форме заявок на участие в торгах и иных документов, представляемых заявителями, с использованием сертифицированных в установленном законодательством Российской Федерации порядке средств криптографической защиты информации.
		6. Оператор ЭП должен обеспечивать создание, обработку, хранение и представление в электронной форме информации и документов, в том числе протоколов комиссии о результатах проведения торгов. Обеспечивать хранение в электронной форме указанных документов в течение десяти лет с даты утверждения протокола о результатах проведения торгов.
		7. Оператор ЭП должен обеспечивать защиту информации, содержащейся в заявках на участие в торгах, иных документах, представляемых участниками торгов, в том числе сохранность этой информации, предупреждение и пресечение уничтожения информации, ее несанкционированные изменение и копирование, нарушения штатного режима обработки информации, включая технологическое взаимодействие с другими информационными системами, в том числе путем применения мер по защите информации, обеспечивающих:

защиту информации, содержащейся на электронной площадке, от несанкционированного доступа;

антивирусную защиту;

обнаружение (предотвращение) вторжений;

целостность электронной площадки и информации, в том числе резервное копирование и восстановление информации;

доступность информации, в том числе защиту электронной площадки от угроз безопасности информации, направленных на отказ в обслуживании электронной площадки.

Защита информации осуществляется в соответствии с установленными законодательством Российской Федерации требованиями о защите информации, содержащейся в государственных информационных системах.

* + 1. Оператор ЭП должен обеспечивать использование сертифицированных в установленном законодательством Российской Федерации порядке средств защиты информации, средств криптографической защиты информации в отношении документов, представленных заявителями и участниками торгов и хранящихся в электронной форме в программно-аппаратном комплексе электронной площадки.

Для целей обеспечения защиты информации от несанкционированного доступа, изменения данных системных внутренних журналов, журналов приема заявок, защиты от вмешательства в системы передачи данных в ходе торгов как со стороны внутренних пользователей (администратор системы, операторы), так и со стороны внешних (участники торгов), оператор электронной торговой площадки обязан использовать сертифицированное в установленном порядке для защиты от указанных способов изменения информации программное обеспечение.

* + 1. Оператор ЭП должен обеспечивать возможность применения организатором торгов, лицами, представившими заявки на участие в торгах, а также участниками торгов средств электронной цифровой подписи.
		2. Оператор ЭП должен обеспечивать конфиденциальность средств идентификации организаторов торгов, лиц, представивших заявки на участие в торгах, участников торгов.
		3. Оператор ЭП должен обеспечивать применение средств антивирусной защиты.
		4. Оператор ЭП должен обеспечивать представление в порядке и в случаях, предусмотренных законодательством Российской Федерации, информации и документов, связанных с проведением торгов и размещаемых на электронной площадке, в том числе сведений, подлежащих опубликованию в соответствии с законодательством Российской Федерации о несостоятельности (банкротстве).
		5. Оператор ЭП должен обеспечивать своевременное представление в Единый федеральный реестр сведений о банкротстве сведений о проведении торгов, подлежащих включению в указанный реестр.
		6. Оператор ЭП должен обеспечивать резервное копирование и восстановление информации.
		7. Оператор ЭП должен использовать программный комплекс, обеспечивающий возможность работы на электронной площадке одновременно зарегистрированных и не зарегистрированных на ней лиц, а также обеспечивающий возможность работы на электронной площадке зарегистрированным на электронной площадке лицам вне зависимости от числа обращений к электронной площадке не зарегистрированных на электронной площадке лиц.
		8. Оператор ЭП должен обеспечить наличие канала связи, позволяющего одновременно принимать участие в работе электронной площадки не менее чем пятистам пользователям, зарегистрированным на электронной площадке, и пятистам пользователям, не зарегистрированным на электронной площадке, со временем ответа на обращение к электронной площадке не более 3000мс.
		9. Оператор ЭП должен обеспечивать электронный документооборот на электронной площадке согласно следующим правилам:

а) все документы и сведения, связанные с получением регистрации на электронной площадке и проведением торгов, направляются участником торгов, организатором торгов, оператором электронной площадки либо размещаются ими на электронной площадке в форме электронных документов;

б) документы и сведения, направляемые в форме электронных документов либо размещаемые указанными лицами на электронной площадке в форме электронных документов, должны быть подписаны усиленной квалифицированной электронной подписью соответственно участника торгов, организатора торгов, оператора электронной площадки;

в) с момента размещения информации, связанной с проведением торгов, в Едином федеральном реестре сведений о банкротстве и на электронной площадке такая информация должна быть доступна для ознакомления на указанном Едином реестре и на электронной площадке без взимания платы.

* 1. Требования к электронным площадкам.
		1. Информационная система оператора электронной площадки для проведения торгов в электронной форме должна быть аттестована в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области защиты информации и персональных данных, предъявляемым к информационным системам не ниже второго класса защищенности «К2» в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждёнными Приказом Федеральной службы по техническому и экспортному контролю от «11» февраля 2013 г. № 17, а также не ниже второго уровня защищенности «УЗ 3» персональных данных в соответствии с «Требованиями о защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Приказом Федеральной службы по техническому и экспортному контролю от «18» февраля 2013 г. № 21.
		2. Электронная площадка должна обеспечивать возможность проведения торгов в соответствии с Порядком проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, утвержденным Приказом Минэкономразвития РФ №495 от 23.07.2015 года, (далее - порядок проведения торгов).
		3. Доступ к электронной площадке через сеть «Интернет» должен быть открытым.
		4. Вся информация на электронной площадке должна размещаться на русском языке, кроме случаев, предусмотренных пунктом 3.2.5. Использование латинских и иных символов и букв при написании русских слов не допускается.
		5. Использование в информации, размещаемой на электронной площадке, букв и символов иностранных языков допускается только в случаях, когда использование букв и символов русского языка приводит к искажению такой информации, в частности при указании адресов сайтов в сети «Интернет», адресов электронной почты.
		6. Электронная площадка должна обеспечивать равные возможности доступа всех лиц к участию в торгах, в том числе к информации о проведении торгов, без взимания с них платы.
		7. Электронная площадка должна обеспечивать наличие у каждого зарегистрированного на электронной площадке лица рабочего раздела на этой площадке («личный кабинет»), доступ к которому может иметь только указанное лицо.
		8. Электронная площадка должна обеспечивать наличие административного раздела, доступ к которому может иметь только оператор электронной площадки.
		9. Электронная площадка должна функционировать в режиме круглосуточной непрерывной работы в течение семи дней в неделю, за исключением времени проведения профилактических работ.

Информация о плановых профилактических работах, во время проведения которых не осуществляется работа электронной площадки, должна быть размещена на электронной площадке не позже чем за сорок календарных дней до даты начала проведения таких работ. При этом период проведения профилактических работ не должен совпадать со временем проведения торгов.

Электронная площадка должна обеспечивать автоматическое уведомление о сроках проведения профилактических работ на электронной площадке, во время которых электронная площадка не функционирует, всех зарегистрированных на электронной площадке лиц путем направления указанным лицам сообщения по электронной почте в срок не позднее чем за сорок дней до даты начала проведения таких работ.

* + 1. Электронная площадка должна обеспечивать доступ к размещаемой на электронной площадке информации посредством использования распространенных веб-обозревателей, в том числе: Internet Explorer 8.0 и выше, Mozilla FireFox 12.0 и выше, Google Chrome 28.0 и выше, Opera 18.0 и выше, Safari 5.0 и выше.
		2. Электронная площадка должна обеспечивать обслуживание не менее 50000 http-запросов в час к любым веб-страницам электронной площадки. Среднее время реакции программного обеспечения от момента поступления http-запроса до момента начала отправки запрошенных данных не должно превышать 1500 мс. Время такой реакции при нагрузке, не превышающей 50000 http-запросов в час, к любым веб-страницам электронной площадки не должно превышать 7000 мс (за исключением случаев возникновения технических сбоев в работе электронной площадки в результате действий третьих лиц).
		3. Электронная площадка должна обеспечивать одновременное участие в работе электронной площадки не менее чем пятисот пользователей, зарегистрированных на электронной площадке, и пятисот пользователей, не зарегистрированных на электронной площадке, со временем ответа на обращение к электронной площадке не более 3000 мс. Работа на электронной площадке зарегистрированных на электронной площадке лиц должна обеспечиваться вне зависимости от числа обращений к электронной площадке не зарегистрированных на электронной площадке лиц (за исключением случаев возникновения технических сбоев в работе электронной площадки в результате действий третьих лиц).
		4. Непрерывность проведения торгов на Электронной площадке должна быть обеспечена, в том числе посредством использования независимо расположенных и имеющих отдельные каналы связи основного и резервного серверов, за счёт бесперебойности функционирования программных и технических средств, используемых для проведения торгов (за исключением случаев возникновения технических сбоев в работе электронной площадки в результате действий третьих лиц).

Серверы, используемые для функционирования электронной площадки, должны располагаться на территории Российской Федерации;

* + 1. Электронная площадка должна обеспечивать создание, обработку и хранение в электронной форме заявок на участие в торгах и иных документов, представляемых заявителями, участниками торгов, а также протоколов о результатах проведения торгов в соответствии с порядком проведения торгов. Обеспечивать хранение в электронной форме указанных документов в течение десяти лет с даты подписания протокола о результатах проведения торгов.
		2. Электронная площадка должна обеспечивать возможность представления электронных документов и применения средств усиленной квалифицированной электронной подписи в соответствии с порядком проведения торгов, сертификат ключа проверки которой выдан любым удостоверяющим центром, аккредитованным в порядке, установленном Федеральным законом от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
		3. Электронная площадка должна обеспечивать возможность автоматической выгрузки информации в ЕФРСБ.
		4. Сведения о соответствии электронной площадки требованиям, указанным в пунктах 3.2.2. -3.2.16, должны содержаться во внутреннем регламенте электронной площадки.
		5. Структура информационной системы электронной площадки должна соответствовать схеме, приведенной на рисунке:



###

### Оборудование

* основной сервер;
* резервный сервер;
* маршрутизаторы;
* коммутаторы;
* АРМ администратора информационной безопасности;
* АРМы операторов электронной площадки;
* АРМы пользователей электронной площадки.

###

### Каналы связи

* Основной канал связи (Интернет провайдер 1);
* Резервный канал связи (Интернет провайдер 2);
* Зашифрованный канал связи

###

### Системное программное обеспечение

* Серверное системное программное обеспечение: операционные системы семейства Microsoft Windows Server или Unix-подобные операционные системы.
* Системное программное обеспечение на АРМах: операционные системы семейства Microsoft Windows или Unix-подобные операционные системы.
* Системное программное обеспечение на коммутационном оборудовании: Unix-подобные операционные системы.

###

### Прикладное программное обеспечение

* Прикладное программное обеспечение на серверах: web-сервер, СУБД, специальное программное обеспечение системы для проведения электронных торгов, крипто-провайдер.
* Прикладное программное обеспечение на АРМах: программное обеспечение для работы с документами в форматах doc, docx, pdf, xls, xlsx, jpg, jpeg, rar, zip и т.д., крипто-провайдер.

### Средства защиты информации

* Средства защиты информации для серверов: средство защиты от несанкционированного доступа, антивирус, крипто-провайдер.
* Средства защиты информации для АРМ администратора информационной безопасности и операторов электронной площадки: средство защиты от несанкционированного доступа, антивирус, крипто-провайдер, VPN-клиент.
* Средства защиты информации для АРМ пользователей: антивирус, крипто-провайдер.
* Межсетевые экраны
* Системы обнаружения вторжений
* Криптошлюзы

	+ 1. Должны выполняться типовые требования к обработке и обеспечению безопасности информации для электронных площадок:

| **№** | **Требование** |
| --- | --- |
| 1. Идентификация и аутентификация субъектов доступа и объектов доступа
 |
|  | Идентификация и аутентификация пользователей, являющихся работниками оператора |
|  | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
|  | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
|  | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
|  | Защита обратной связи при вводе аутентификационной информации |
|  | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| 1. Управление доступом субъектов доступа к объектам доступа
 |
| 1.
 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
|  | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
|  | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
|  | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
|  | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
|  | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
|  | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
|  | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
|  | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
|  | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
|  | Регламентация и контроль использования в информационной системе мобильных технических средств |
|  | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
|  | Обеспечение доверенной загрузки средств вычислительной техники |
| 1. Ограничение программной среды
 |
| 1.
 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
|  | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |
| 1. Защита машинных носителей информации
 |
| 1.
 | Учет машинных носителей информации |
|  | Управление доступом к машинным носителям информации |
|  | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
|  | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |
| 1. Регистрация событий безопасности
 |
| 1.
 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
|  | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
|  | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
|  | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
|  | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
|  | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
|  | Защита информации о событиях безопасности |
| 1. Антивирусная защита
 |
| 1.
 | Реализация антивирусной защиты |
|  | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| 1. Обнаружение вторжений
 |
| 1.
 | Обнаружение вторжений |
|  | Обновление базы решающих правил |
| 1. Контроль (анализ) защищенности информации
 |
| 1.
 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
|  | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
|  | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
|  | Контроль состава технических средств, программного обеспечения и средств защиты информации |
|  | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе |
| 1. Обеспечение целостности информационной системы и информации
 |
| 1.
 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
|  | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |
|  | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| 1.
 | Использование отказоустойчивых технических средств |
|  | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| 1. Обеспечение доступности информации
 |
|  | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
|  | Периодическое резервное копирование информации на резервные машинные носители информации |
|  | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
|  | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| 1. Защита среды виртуализации
 |
| 1.
 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
|  | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
|  | Регистрация событий безопасности в виртуальной инфраструктуре |
|  | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
|  | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
|  | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
|  | Контроль целостности виртуальной инфраструктуры и ее конфигураций |
|  | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
|  | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
|  | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| 1. Защита технических средств
 |
| 1.
 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
|  | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены |
|  | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| 1. Защита информационной системы, ее средств, систем связи и передачи данных
 |
| 1.
 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
|  | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
|  | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
|  | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
|  | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
|  | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
|  | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
|  | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
|  | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
|  | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
|  | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
|  | Защита беспроводных соединений, применяемых в информационной системе |
|  | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
|  | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
|  | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |

1. **Порядок подтверждения соответствия**

**оператора электронной площадки условиям членства в Союзе**

 **при проведении плановой проверки**

* 1. В рамках осуществления плановой проверки Рабочим органом Союза, обеспечивающим контроль за деятельностью его членов, оператор электронной площадки – член СТЭП предоставляет в Контрольный комитет документы, предусмотренные п.п. 2.7.1. – 2.7.20. ПРАВИЛ ПРИЁМА В ЧЛЕНЫ СОЮЗА ТОРГОВЫХ ЭЛЕКТРОННЫХ ПЛОЩАДОК И ПРЕКРАЩЕНИЯ ЧЛЕНСТВА В СОЮЗЕ.
	2. Периодичность плановых проверок установлена в Графике проведения плановых проверок .
	3. Документы предоставляются по запросу Контрольного комитета или Дисциплинарной комиссии в течение 5 (пять) рабочих дней с момента поступления такого запроса. Документы должны быть представлены в читаемом виде, сшиты, пронумерованы, заверены печатью юридического лица (индивидуального предпринимателя) – оператора электронной площадки.
	4. Контрольный комитет Союза, обеспечивающий контроль за деятельностью его членов в течение 10 (десяти) рабочих дней принимает решение о соответствии электронных площадок и операторов электронных площадок (документы которых поступили на рассмотрение) требованиям, установленным Законом о банкротстве, условиям членства в Союзе. В случае затруднения при принятии решения о соответствии сроки рассмотрения документов могут быть продлены, но не более чем на 10 (десять) рабочих дней.

По представлению Директора Союза Решение Контрольного комитета Союза о соответствии электронных площадок и операторов электронных площадок может быть пересмотрено Дисциплинарной комиссией  в течение 10 (десяти) рабочих дней с момента принятия такого решения.