Приложение 1

УТВЕРЖДЕНА

приказом НИУ ВШЭ

от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ИНСТРУКЦИЯ**

**по обращению со средствами криптографической защиты информации при работе на электронной площадке автоматизированной системы торгов государственного оборонного заказа в Национальном исследовательском университете «Высшая школа экономики»**

* 1. **Общие положения**

1.1. Инструкция по обращению со средствами криптографической защиты информации в Национальном исследовательском университете «Высшая школа экономики» (далее соответственно – Инструкция, СКЗИ, НИУ ВШЭ) разработана в целях регламентации действий лиц, допущенных к работе с СКЗИ в НИУ ВШЭ, которые осуществляют работы с применением СКЗИ.

1.2. Под работами с применением СКЗИ в Инструкции понимается защищенное подключение к автоматизированной системе торгов государственного оборонного заказа, подписание электронных документов усиленной квалифицированной электронной подписью (далее – УКЭП) и проверка подписи, шифрование файлов другие действия согласно технической документации на СКЗИ.

Под обращением с СКЗИ в Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

1.3. Инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

1.4. Инструкция в своем составе, терминах и определениях основывается на положениях Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи", Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152 (далее – Инструкция ФАПСИ от 13.06.2001 № 152), Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (далее – Положение ПКЗ-2005), утвержденного приказом ФСБ РФ от 09.02.2005 № 66, а также Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ от 10.07.2014 № 378.

* 1. **Термины и определения**

2.1. Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

2.2. Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

2.3. Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

2.4. Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

2.5. Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

2.6. Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

2.7. Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

2.8. Орган криптографической защиты (ОКЗ) – структурное подразделение НИУ ВШЭ, работник НИУ ВШЭ или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлению мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

2.9. Ответственный за организацию работ по криптографической защите информации (Ответственный) – работник НИУ ВШЭ, отвечающий за реализацию мероприятий, связанных с обеспечением в НИУ ВШЭ безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

2.10. Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений УКЭП, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

2.11. УКЭП – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

* 1. **Порядок получения допуска пользователей к работе с СКЗИ**

3.1. Для получения допуска к работе с СКЗИ работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний.

3.2. Основанием для допуска пользователя к работе с СКЗИ является внесение его в перечень пользователей СКЗИ, утверждаемый старшим директором по цифровой трансформации НИУ ВШЭ.

3.3. Контроль реализации данных мероприятий возлагается на Ответственного.

* 1. **Работа с СКЗИ**

4.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей в присутствии посторонних лиц запрещены. В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

4.2. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть промаркированы и должны использоваться, учитываться и храниться в общем порядке. Все копии учитываются за отдельным номером.

4.3. Каждый ключевой документ должен быть зарегистрирован в Журнале поэкземплярного учета СКЗИ.

4.4. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только с разрешения руководителя организации с соответствующей пометкой в журнале поэкземплярного учета.

4.5. При обнаружении на рабочей станции с установленным СКЗИ программного обеспечения, не соответствующего объему и сложности решаемых задач на данном рабочем месте, а также вирусных программ, незамедлительно должны быть организованы работы по расследованию инцидента информационной безопасности.

* 1. **Действия в случае компрометации ключей**

5.1. О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической защите информации.

5.2. К компрометации ключей относятся следующие события:

* + 1. утрата носителей ключа;
		2. утрата иных носителей ключа с последующим обнаружением;
		3. возникновение подозрений на утечку ключевой информации или ее искажение;
		4. нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
		5. утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
		6. утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
		7. доступ посторонних лиц к ключевой информации;
		8. другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

5.3. В случае компрометации ключа пользователя незамедлительно должны быть приняты меры по отзыву ключа (отзыв сертификата УКЭП в удостоверяющем центре, обновление списков отозванных сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации.

5.4. Визуальный осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

5.5. Расследование инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет обладатель скомпрометированной информации ограниченного доступа. При необходимости привлекается орган криптографической защиты.

* 1. **Ответственность лиц, допущенных к работе с СКЗИ**

6.1. За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.