ПРИЛОЖЕНИЕ № 6

к протоколу заседания подкомиссии

по использованию информационных технологий

при предоставлении государственных

и муниципальных услуг

Правительственной комиссии

по использованию информационных технологий

для улучшения качества жизни и условий ведения

предпринимательской деятельности

от 23 июня 2017 г. № \_\_\_\_

ОДОБРЕНО

подкомиссией по использованию информационных технологий при предоставлении государственных

и муниципальных услуг

Правительственной комиссии

по использованию информационных технологий

для улучшения качества жизни и условий ведения

предпринимательской деятельности
(протокол от 23 июня 2017 г. №\_\_\_)

**РЕКОМЕНДОВАННЫЕ ТРЕБОВАНИЯ**

**к минимальной функциональности средств защиты информации рабочих мест пользователей, осуществляющих информационное взаимодействие с региональной информационной системой «Контингент обучающихся» субъекта Российской Федерации**

**Москва**

**2017 г.**

Оглавление

[1 Аннотация 3](#_Toc478448787)

[2 Перечень сокращений 4](#_Toc478448788)

[3 Термины и определения 5](#_Toc478448789)

[4 Принципы и правила обработки персональных данных в ИС «Контингент обучающихся» 6](#_Toc478448790)

[5 Требования по обеспечению информационной безопасности рабочих мест 7](#_Toc478448791)

[6 Ответственность 12](#_Toc478448792)

# Аннотация

Целью разработки данных Требований является определение функциональных характеристик, предъявляемых к средствам защиты информации рабочего места пользователя, с которого осуществляется информационное взаимодействие (непосредственное, либо посредством иных информационных систем) с региональной информационной системой «Контингент обучающихся» субъекта Российской Федерации. Данные требования разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных», приказами ФСТЭК № 17 от 11 февраля 2013 года и № 21 от 18 февраля 2013 года, а также «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119, и определяют принципы обработки и обеспечения безопасности персональных данных в ИС «Контингент обучающихся»**.**

# Перечень сокращений

| Сокращение | Расшифровка сокращения |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ПДн | Персональные данные |
| НСД | Несанкционированный доступ |
| ИС | Информационная система |
| ИСПДн | Информационная система персональных данных |
| ГИС «Контингент обучающихся» | Государственная информационная система «Контингент обучающихся» субъекта Российской Федерации |
| ФИС «Контингент обучающихся» | Федеральная информационная система «Контингент обучающихся» |
| ИС «Контингент обучающихся» | Информационные системы, включающие в себя как государственные информационные системы «Контингент обучающихся» субъекта Российской Федерации, так и ФИС «Контингент обучающихся». |

# Термины и определения

| Термин | Определение термина |
| --- | --- |
| автоматизированная обработка персональных данных | обработка персональных данных с помощью средств вычислительной техники |
| доступ к информации | возможность получения информации и ее использования |
| информационная система персональных данных | совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств |
| обработка персональных данных | любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных |
| персональные данные | любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) |
| трансграничная передача персональных данных | передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу |

# Принципы и правила обработки персональных данных в ИС «Контингент обучающихся»

4.1. Обработка персональных данных в ИС «Контингент обучающихся» осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых в системе персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

4.2. При обработке персональных данных в ИС «Контингент обучающихся» обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. Владельцами системы принимаются необходимые меры по удалению или уточнению неполных или неточных персональных данных.

4.3. Хранение персональных данных в системе осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, либо по достижению максимального срока хранения в ИС «Контингент обучающихся», если иное не предусмотрено федеральным законом.

4.4. В ИС «Контингент обучающихся» не обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

4.5. В системе не осуществляется трансграничной передачи персональных данных и не принимается решений в отношении субъекта персональных данных, основанных исключительно на автоматизированной обработке.

4.6. Хранение всех персональных данных, используемых в ИС «Контингент обучающихся» осуществляется только на территории Российской Федерации.

4.7. Минимально допустимый класс защищенности ИС «Контингент обучающихся» субъекта Российской Федерации не ниже К2.

4.8. Установить необходимость обеспечения второго уровня защищенности персональных данных при их обработке в ИС «Контингент обучающихся» субъекта Российской Федерации.

4.9. Определить необходимость применения мер защиты информации, соответствующих требованиям класса К2, достаточными, т.к. применяемые меры защиты информации удовлетворяют требованиям по обеспечению 2-го уровня защищенности информационных систем персональных данных.

# Требования по обеспечению информационной безопасности рабочих мест

Настоящие требования предъявляются ко всем автоматизированным рабочим местам пользователей, осуществляющих информационное взаимодействие с государственной информационной системой «Контингент обучающихся» субъекта Российской Федерации.

Состав настоящих требований основан на предположении, что на АРМ пользователя может сохраняться информация, полученная из системы, либо передаваемая в систему. Соответственно данные требования должны быть реализованы до момента подключения АРМ пользователя к ГИС «Контингент обучающихся» и не требовать изменения уже существующей архитектуры сети, созданной в субъекте Российской Федерации.

В целях обеспечения соответствующего уровня информационной безопасности ГИС «Контингент обучающихся» все АРМ пользователей, взаимодействующие с данной системой должны быть обеспечены следующим минимальным набором средств защиты:

* средство защиты от НСД;
* средство антивирусной защиты;
* средство защиты от сетевых атак;
* средство защиты при доступе к web приложениям.

Данный набор средств минимально необходим, но в отдельных случаях может быть дополнен в соответствии с принятыми моделями угроз и нарушителя безопасности информации, а также по решению оператора государственной информационной систем «Контингент обучающихся» субъекта Российской Федерации.

* 1. Требования по средствам защиты от НСД

Средства защиты АРМ пользователей от НСД должны обеспечивать следующие функции:

* защиту АРМ пользователя от НСД;
* контроль входа пользователя в систему, в том числе и с использованием дополнительных аппаратных средств защиты;
* сквозная аутентификация по аппаратным идентификаторам;
* возможность блокировки сессии пользователя по периоду неактивности;
* разграничение доступа пользователя к устройствам и контроль аппаратной конфигурации АРМ;
* разграничение доступа пользователей к информации;
* контроль утечек информации;
* избирательное (дискреционное) управление доступом:
	+ возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;
	+ возможность наследования прав доступа для файлов и каталогов;
	+ возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту;
* полномочное (мандатное) управление доступом:
	+ возможность выбора уровня конфиденциальности сессии для пользователя;
	+ возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;
	+ возможность изменения количества мандатных меток в системе и их названий;
	+ контроль потоков конфиденциальной информации в системе;
	+ возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP;
* Контроль вывода конфиденциальных данных на печать
* Контроль аппаратной конфигурации компьютера и подключаемых устройств
* поддержка персональных идентификаторов iButton; USB-ключей eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ, iKey 2032, Rutoken/Rutoken S, Rutoken ЭЦП, Rutoken Lite; смарт-карт eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ, ESMART Token для входа в систему и разблокировки компьютера;
* Возможность ограничить работу сетевого интерфейса заданными уровнями конфиденциальности сессий;
* возможность блокирования входа в систему локальных пользователей;
* возможность блокирования операций вторичного входа в систему в процессе работы пользователей;
* Контроль целостности файлов, каталогов, элементов системного реестра;
* Возможность блокировки компьютера при подключении или отключении заданных устройств;
* Возможность обновления ПО с электронной подписью без необходимости корректировки настроек контроля целостности;
* Блокировка запуска при нарушении целостности контролируемых модулей;
* Затирание файлов небольшого размера;
* Затирание данных в файловой системе ReFS;
* Возможность интеграции компьютеров, работающих под управлением ОС GNU/Linux, в общую инфраструктуру управления и мониторинга;
* Регистрацию событий безопасности в журнале;
	+ Должна быть возможность формирования отчетов по результатам аудита;
	+ Должна быть возможность поиска и фильтрации при работе с данными аудита;
	+ Разделение событий НСД на просмотренные и новые;

Используемые средства защиты от НСД должно соответствовать требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности. Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля.

6.2. Требования к средствам антивирусной защиты

Антивирусные средства защиты АРМ пользователей должны обеспечивать следующие функции:

* автоматическую проверку наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа;
* сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию;
* удаление вредоносного программного обеспечения и его блокировку (перемещение в “карантин”);
* откат операций удаления программного обеспечения, воспринятого как вредоносное;
* должно обеспечивать кэширование данных сканирования для сокращения времени обнаружения вредоносного программного обеспечения;
* должен обеспечиваться контроль целостности компонентов для защиты модулей продукта, включая антивирусные базы и базы правил от подмены;
* возможность обновления антивирусных баз;
* регистрацию событий безопасности.

Средства антивирусной защиты должно соответствовать: требованиями руководящего документа "Требования к средствам антивирусной защиты" (утвержден приказом ФСТЭК России от 20 марта 2012 г. № 28) для типов "А", "Б", "В" и "Г" по 5-му классу защиты.

* 1. Требования к средствам обнаружения (предотвращения) вторжений.

Средства защиты АРМ пользователей от сетевых атак должны обеспечивать следующие функции:

* контроль входящих и исходящих соединений;
* контроль для приложений, использующихся на АРМ, при обращении к сети и создание правил сетевого доступа для приложений;
* режим обучения для сетевого доступа для приложений;
* должно обеспечивать блокировку сетевых сканеров;
* должна быть возможность задать список доверенных узлов и портов;
* должно иметь возможность интеграции с межсетевым экраном;
* должно обеспечивать непрерывный мониторинг;
* регистрацию событий безопасности.

Средство обнаружения (предотвращения) вторжений должно иметь действующий сертификат ФСТЭК в соответствии с требованиями руководящего документа «Требования к системам обнаружения вторжений», утвержденного приказом ФСТЭК России от 6 декабря 2011г. №638 не ниже, чем по 5 классу защиты СОВ (ИТ.СОВ.У5.ПЗ).

* 1. Требования к средствам межсетевого экранирования

Средства межсетевого экранирования АРМ пользователей должны обеспечивать следующие функции:

* должно контролировать входящие и исходящие соединения;
* должно определять правила для всех процессов, запущенных в системе, правила передачи данных и контролировать ICMP-трафик системы;
* должно обеспечивать контроль для приложений, использующихся на компьютере, при обращении к сети и создание правил сетевого доступа для приложений;
* режим обучения для сетевого доступа для приложений;
* разделение доступа к узлам сети;
* создание разрешенного и запрещенного списков сетевых ресурсов;
* должна быть возможность фильтрации всех входящих/исходящих интернет- соединений по IP-адресам;
* возможность экспорта/импорта настроек межсетевого экрана с одного компьютера на другой;
* должно обеспечивать регистрацию событий безопасности;
* должен иметь возможность интеграции со средством обнаружения вторжений;

Средство межсетевого экранирования должно иметь сертификат ФСТЭК в соответствии с Приказом ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам не ниже, чем по 5-му классу защиты.

* 1. Требования к средствам защиты при доступе к web приложениям

Средства защиты АРМ пользователей при доступе к web приложениям должны обеспечивать следующие функции:

        реализация TLS-аутентификации (в том числе односторонней) на основе технологии открытых ключей (используются сертификаты открытых ключей стандарта X.509 версии 3, совместимые с Удостоверяющим центром "КриптоПро");

        установление защищенного соединения с сервером на базе протокола HTTPS, в том числе по выделенному TLS-туннелю, и обмен данными с ресурсами корпоративной сети;

  возможность работы с серверами, поддерживающими протокол TLS v. 1.0, TLS v 1.2;

        хранение ключевой информации в защищенном контейнере;

        проверка сертификатов ключей по списку отозванных сертификатов;

        регистрация событий, связанных с настройкой и функционирование средств защиты АРМ пользователей при доступе к web-приложениям;

        контроль целостности программного обеспечения, передаваемой и хранимой информации;

        очистка сессионной, включая криптографическую, информацию при разрыве соединения.

Средства защиты при доступе к web приложениям должно соответствовать требованиям ГОСТ 28147-89, ГОСТ Р 34.11.-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11.2012, требованиям ФСБ России к шифровальным (криптографическим) средствам класса не ниже КС2 и иметь возможность использования для криптографической защиты (создание и управление ключевой информацией, шифрование и имитозащита данных, передаваемых в IP-пакетах по общим сетям передачи данных, криптографическая аутентификация абонентов при установлении соединения) информации, не содержащей сведений, составляющих государственную тайну.

# Ответственность

Ответственность за выполнение настоящих Требований возлагается на назначенное лицо организаций, осуществляющих образовательную деятельность, чьи сотрудники подключаются к ГИС «Контингент обучающихся» согласно принятым в организации организационно-распорядительным документациям в области защиты информации.