Меры по защите информации в информационной системе «Управление бюджетным процессом Ленинградской области»

1. Общие положения

Информационная система «Управление бюджетным процессом Ленинградской области» (ИС УБП ЛО) является государственной информационной системой. В подсистеме оплаты труда ИС УБП ЛО может вестись обработка персональных данных.

ИС УБП ЛО аттестована по 3 классу защищенности, в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Перечень документов, на основании которых выполняются мероприятия по информационной безопасности в ИС УБП ЛО приведён в таблице 1.

Таблица 1

Наименование документа
Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»
Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении 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»
Приказ ФАПСИ от 13 июня 2001 г.№152 «Об утверждении 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»
Приказ ФСТЭК России от 11 февраля 2013 № 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в

государственных информационных системах
Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России) от 18 февраля 2014 г. № 21 об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

2. Организационные мероприятия по защите информации

Организационными мерами по обеспечению безопасности ИС УБП ЛО являются:

- определение лиц, ответственных за информационную безопасность, администраторов информационной безопасности, администраторов;
- ограничение доступа к техническим средствам и средствам информационной безопасности;
- обеспечение режима безопасности помещений, в которых размещена система;
- обеспечение сохранности носителей информации;
- разграничение доступа к данным;
- определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;
- учет средств защиты информации;
- обучение специалистов, ответственных за информационную безопасность и пользователей;
- информирование пользователей об актуальных угрозах безопасности;
- проведение внутренних контрольных мероприятий.

3. Технические мероприятия по защите информации

В качестве технических мер для управления защитой и обеспечения безопасности ИС УБП ЛО необходимо:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;

- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

4. Требования к типовым автоматизированным рабочим местам, подключаемым к подсистеме оплаты труда ИС УБП ЛО

Автоматизированные рабочие места, подключаемые к подсистеме оплаты труда ИС УБП ЛО, должны быть аттестованы в соответствии с требованиями к защите информации.

Организационные меры при работе в ИС УБП ЛО определяются организационно-распорядительными документами, приведенными в Таблице 2.

Таблица 2

Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе Назначении структурного подразделения или должностного лица (работника), ответственных за защиту информации, содержащейся в информационной системе	п. 14. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" п. 16 Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении 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" п. 9 Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной	п. 13 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

системе, необходим для выполнения ими служебных (трудовых) обязанностей	п. 8 Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении 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"
Правила доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях	п. 13 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" п. 6 Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении 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"
Перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ	п. 6 Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении 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"
Правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных	пп.8, п.2, ст. 19 Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных" п. 8.2 Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

Определение границ контролируемой зоны	п. 10 Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении 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" ЗИС.3 Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
Журнал учета носителей персональных данных с использованием регистрационных (заводских) номеров	п. 7 Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении 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" ЗНИ.1 Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Контроль за выполнением требований к защите персональных данных при их обработке в информационной системе	п. 2 ст 18.1 Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" п. 17 постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
Правила разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и вве-	п. 15.1 Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" п. 16.3 Приказ ФСТЭК России от 11.02.2013 N 17 "Об

дение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;	утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Правила генерации и смены паролей пользователей	АНЗ.5 Приказ ФСТЭК России от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Журнал учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)	п. 26 Приказ ФАПСИ от 13.06.2001 N 152 "Об утверждении 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"
Перечень пользователей СКЗИ	п. 19 Приказ ФАПСИ от 13.06.2001 N 152 "Об утверждении 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"
Заключение о возможности эксплуатации СКЗИ	п. 7 Приказ ФАПСИ от 13.06.2001 N 152 "Об утверждении 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"
Заключение об обучении пользователей правилам работы с СКЗИ	п. 21 Приказ ФАПСИ от 13.06.2001 N 152 "Об утверждении 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"

Средства защиты информации, применяемые в ИС УБП ЛО, должны иметь сертификаты соответствия требованиям по безопасности информации, подтверждающим возможность их применения в государственных информационных системах не ниже 3 класса защищенности (К3).

На типовых рабочих местах, подключаемых к ИС УБП ЛО, должны применяться:

- средства антивирусной защиты не ниже 6 класса («Требования к средствам антивирусной защиты» Утверждены приказом ФСТЭК России от 20 марта 2012 № 28 ДСП);
- средства защиты информации от несанкционированного доступа;
- межсетевые экраны не ниже 6 класса («Требования к межсетевым экранам», утверждены приказом ФСТЭК России от 9 февраля 2016 г. №9, ДСП);
- средства криптографической защиты информации не ниже класса КС1.