УТВЕРЖДЕНО
решением Совета директоров
ООО «Управление Сбережениями»
Протокол № 10 от 30.06.2016 года.
Введено в действие с 30.06.2016 г.
Приказ № 17/16 от 30.06.2016 г.
Генеральный директор
ООО «Управление Сбережениями»

_____/Кузнецов С.Э.

Перечень мер ООО «Управление Сбережениями» по обеспечению безопасности персональных данных при их обработке
(новая редакция)

Москва – 2016 г.

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Настоящий перечень мер Общества с ограниченной ответственностью «Управление Сбережениями» (далее – Компания) по обеспечению безопасности персональных данных при их обработке (далее – Перечень) разработан во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон) и иных нормативных правовых актов Российской Федерации в области регулирования отношений, связанных с обработкой персональных данных.

1.2. Настоящий Перечень распространяется на отношения, возникающие при обработке персональных данных как с использованием информационных систем персональных данных, так и без использования таковых.

1.3. Для целей настоящего Перечня используются следующие основные определения и понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) 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;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

12) уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных

угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Основные принципы обеспечения безопасности персональных данных

2.1. Система обеспечения безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, включает в себя проведение следующих мероприятий:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) внедрение организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

3) осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;

4) осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Определение угроз безопасности персональных данных при их обработке.

3.1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы безопасности персональных данных.

3.2. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе персональных данных, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия

3.3. Угрозами безопасности персональных данных, актуальными при их обработке в информационных системах персональных данных Компании с учетом специфики ее деятельности являются угрозы:

- несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;
- воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;
- использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;
- несанкционированного доступа к отчуждаемым носителям персональных данных;
- утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;
- несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;
- несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;
- несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

- несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;

- несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

3.4. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится Компанией с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований к защите персональных данных, установленных Законом и принятыми в соответствии с ним нормативными правовыми актами.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3.5. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

3.5.1. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.5.2. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.5.3. Необходимость обеспечения 3-го уровня защищенности персональных данных при их

обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.5.4. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3.6. Для обеспечения каждого из уровней защищенности персональных данных при их обработке в информационной системе необходимо выполнение нижеприведенных условий.

3.6.1. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

3.6.2. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 4.6.1. настоящего Перечня, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

3.6.3. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 4.6.2 настоящего Перечня, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) Компании, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

3.6.4. Для обеспечения 1-го уровня защищенности персональных данных при их обработке

в информационных системах помимо требований, предусмотренных пунктом 4.6.3. настоящего Перечня, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

3.7. Определения типа угроз, характерных для информационных систем персональных данных, используемых Компанией, а также необходимости применения одного из уровней защищенности персональных данных к каждой из вышеуказанных систем, приведено в Приложении № 1 к настоящему Перечню.

4. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

4.1. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119.

Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

4.2. . В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных..

4.3. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении № 2 к настоящему Перечню.

4.4. Описание мер, применяемых Компанией, с целью обеспечения безопасности персональных данных с учетом необходимого уровня защищенности персональных данных каждой информационной системы персональных данных, используемых Компанией, приведено в Приложении № 3 к настоящему Перечню.

5. Оценки эффективности принимаемых мер по обеспечению безопасности персональных данных.

5.1. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится Компанией самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

5.2. Для проведения оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных Компанией самостоятельно, Генеральный директор Компании приказом назначает инспекционную комиссию, а также руководителя комиссии, из числа сотрудников Компании для проведения такой оценки и срок ее проведения. По результатам проведенной оценки, руководитель комиссии предоставляет Генеральному директору отчет о проведенной оценке, а также рекомендации по повышению эффективности реализуемых мер по обеспечению безопасности персональных данных.

6. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.1. Контроль за выполнением требований законодательства РФ в области защиты персональных данных организуется и проводится Компанией самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые Генеральным директором Компании.

6.2. Ответственность за осуществление внутреннего контроля в соответствии с настоящим Перечнем возлагается на контролера (руководителя службы внутреннего контроля) Компании.

6.3. Контролер (руководитель службы внутреннего контроля) осуществляет текущий контроль, а также проводит периодически проверки соответствия принимаемых Компанией мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных требованиям законодательства Российской Федерации в области защиты персональных данных, настоящего Перечня и иных внутренних документов Компании.

7. Заключительные положения.

7.1. Ответственность за организацию обеспечения безопасности персональных данных при их обработке и ее соответствие требованиям законодательства Российской Федерации в области защиты персональных данных, настоящего Перечня и иных внутренних документов Компании несет Генеральный директор.

7.2. Генеральный директор назначает сотрудника, ответственного за реализацию мер по обеспечению безопасности персональных данных при их обработке.

7.3. Ответственный сотрудник разрабатывает внутренние документы Компании, касающиеся обеспечения безопасности персональных данных при их обработке, вносит предложения по внесению в них изменений, осуществляет оценку используемых Компанией информационных систем персональных данных, определение типа угроз безопасности персональных данных для каждой информационной системы, определяет необходимы уровень защищенности персональных данных, обеспечивает реализацию общих организационных и технических мер по обеспечению безопасности персональных данных, организует проведение оценки и контроля эффективности принимаемых мер по обеспечению безопасности персональных данных.

7.4. Настоящий Перечень доступен для ознакомления на официальном сайте Компании в сети Интернет по адресу: www.sv-mg.ru.

8. Внесение изменений.

8.1. В настоящий Перечень могут быть внесены изменения.

8.2. Инициатором внесения изменений может быть Генеральный директор и/или контролер (руководитель службы внутреннего контроля) Компании и/или ответственный сотрудник.

8.3. Предложения излагаются в письменном виде и подлежат обязательному согласованию с контролером (руководителем службы внутреннего контроля), юридическим отделом, Генеральным директором.

8.4. Новая редакция Перечня подлежит утверждению органами Компании, в компетенцию которых в соответствии с Уставом входит решение вопросов, изложенных в настоящем Перечне.

Приложение № 1

Перечень информационных систем персональных данных, используемых Компанией

Номер п/п	Наименование информационной системы персональных данных	Тип угроз безопасности персональных данных, характерный для информационной системы	Уровень защищенности, требуемый для информационной системы
1	2	3	4
1	Система электронного документооборота (ЭДО) на базе программы 1С	2 (для информационной системы в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе)	3 (для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;)
2	1С: Бухгалтерия: ООО «Управление Сбережениями»	2 (для информационной системы в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе)	3 (для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;)
3	1С: Бухгалтерия: CRM	2 (для информационной системы в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе)	3 (для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;)
4	1С: Бухгалтерия: Паевые инвестиционные фонды	2 (для информационной системы в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе)	3 (для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;)
5	1С: Бухгалтерия: Зарплата и управление персоналом	2 (для информационной системы в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных)	3 (для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории

		возможностей в прикладном программном обеспечении, используемом в информационной системе)	персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;)
6	Личный кабинет на сайте ООО «Управление Сбережениями» по адресу www.sv-mg.ru	2 (для информационной системы в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе)	3 (для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;)

Состав и содержание
мер по обеспечению безопасности персональных данных,
необходимых для обеспечения каждого из уровней
защищенности персональных данных

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной	+	+	+	+

	системе)				
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет,				

	разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	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				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+

VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	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)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					

ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими				

	средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	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, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных 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	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	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				

ЗИС.8	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				
ЗИС.9	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				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о			+	+

	возникновении инцидентов в информационной системе пользователями и администраторами				
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

"+" - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.

Приложение № 3

Описание мер, применяемых Компанией, с целью обеспечения безопасности персональных данных с учетом необходимого уровня защищенности персональных данных каждой информационной системы персональных данных, используемых Компанией

№ п/п	Содержание мер по обеспечению безопасности персональных данных	Описание принимаемых Компанией мер
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
5	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Производится для систем, находящихся в Демилитаризованной зоне (DMZ, ДМЗ), средствами систем, которые расположены в ДМЗ
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
6	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Производится стандартными средствами windows с ролью Active directory (АД, AD)
7	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Производится стандартными средствами windows созданием групп пользователей в АД
8	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Производится на канальном уровне VLAN сетями и защитными экранами на сетевом уровне

9	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Производится стандартными средствами windows разделение прав групп пользователей в АД, разделение прав пользователей для каждой прикладной программы - внутренними средствами самой программы
10	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Производится стандартными средствами windows: - ограничения на файловые ресурсы; - назначение прав группам на исполнение различных видов программного обеспечения; - назначение прав пользователей для каждой прикладной программы внутренними средствами самой программы.
11	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
12	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Производится сервером аутентификации RADIUS(система 4TRESS)
15	Обеспечение доверенной загрузки средств вычислительной техники	Не используется, поскольку локальные ПК (персональные компьютеры) работают в терминальном режиме и не имеют под собой каких - либо важных систем.
III. Ограничение программной среды (ОПС)		
16	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Осуществляется на уровне решения генерального директора по представлению сотрудников отдела информационно-технического обеспечения
17	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	Производится стандартными средствами windows
IV. Защита машинных носителей персональных данных (ЗНИ)		
18	Учет машинных носителей персональных данных	Машинные носители персональных данных не используются
19	Управление доступом к машинным носителям персональных данных	Использование машинных носителей осуществляется на специальных ПК с контролем системой DEVICELOCK
V. Регистрация событий безопасности (РСБ)		
20	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS)
21	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Производится стандартными средствами windows и сервером аутентификации RADIUS(система 4TRESS), а также системой сбора логов, встроенных в прикладное программное обеспечение.
VI. Антивирусная защита (АВЗ)		
22	Реализация антивирусной защиты	Реализовано системой SYMANTEC и Kaspersky Antivirus

23	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Производится от 30 мин до 1 дня в зависимости от системы
VII. Обнаружение вторжений (СОВ)		
24	Обнаружение вторжений	Производится установленными системами антивирусной защиты и стандартными средствами windows
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
25	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Осуществляется на регулярной основе
26	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Осуществляется на регулярной основе
27	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Осуществляется на регулярной основе в тестовой среде
28	Контроль состава технических средств, программного обеспечения и средств защиты информации	Осуществляется на регулярной основе
29	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	Осуществляется на регулярной основе
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)		
30	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Осуществляется на регулярной основе
31	Контроль целостности персональных данных, содержащихся в базах данных информационной системы	Осуществляется на регулярной основе
32	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	Осуществляется на регулярной основе
33	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)	Осуществляется на регулярной основе
34	Ограничение прав пользователей по вводу информации в информационную систему	Реализовано с помощью программных средств
35	Контроль точности, полноты и правильности данных, вводимых в информационную систему	Осуществляется не программными средствами
X. Обеспечение доступности персональных данных (ОДТ)		
36	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы	Осуществляется резервное копирование данных

37	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	Не осуществляется
XI. Защита среды виртуализации (ЗСВ)		
38	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Производится средствами VMWARE
39	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Производится средствами VMWARE
40	Регистрация событий безопасности в виртуальной инфраструктуре	Производится средствами VMWARE
41	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Производится средствами VMWARE
42	Контроль целостности виртуальной инфраструктуры и ее конфигураций	Производится средствами VMWARE
43	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Производится средствами VMWARE и средствами СХД NETAPP
44	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Производится средствами SYMANTEC
45	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Производится средствами VMWARE
XII. Защита технических средств (ЗТС)		
46	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам	Осуществляется
47	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 средств	Производится размещением всего оборудования в помещениях с разграничением и контролем доступа в эти помещения
48	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	Используются средства бесперебойного питания
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
19	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы	Производится на канальном уровне VLAN сетями и защитными экранами на сетевом уровне

50	Обеспечение защиты персональных данных 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	Производиться путем организации защищенного канала данных
51	Использование устройств терминального доступа для обработки персональных данных	Используется
52	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	Осуществляется программными средствами
53	Защита беспроводных соединений, применяемых в информационной системе	Беспроводные соединения не используются
XIV. Выявление инцидентов и реагирование на них (ИНЦ)		
54	Определение лиц, ответственных за выявление инцидентов и реагирование на них	В компании установлены лица, ответственные за реализацию мер по защите персональных данных
55	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Осуществляется, не регламентировано
56	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	Осуществляется, не регламентировано
57	Принятие мер по устранению последствий инцидентов	Осуществляется, не регламентировано
58	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	Осуществляется, не регламентировано
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
29	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Осуществлено в рамках должностных обязанностей сотрудников и разграничений прав доступа на программном уровне
60	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом	Осуществляется, не регламентировано
61	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Осуществляется, не регламентировано