

Административные здания
по адресу: г.Киров, ул.Дерендяева, 77

**СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ
ДОСТУПОМ**

Система защиты персональных данных
Пояснительная записка

1852-СЗИ

2017

Содержание

1. Общие положения	2
2. Нормативно-правовые основания	2
3. Используемые сокращения	3
4. Технологические процессы ИСПДн	3
5. Сегменты ИС и требования безопасности	5
6. Оценка угроз безопасности информации	6
6.1. Уровень исходной защищенности по модели	7
4.2. Выбор актуальных типов нарушителя	10
4.2. Определение актуальных угроз безопасности	12
7. Выбор мероприятий по обеспечению безопасности ПДн	16
Приложение А – определение актуальных угроз	18
Приложение Б – выбор мер информационной безопасности	22
Приложение В – перечень актуальных угроз и нейтрализующих мер	40

Согласовано:

Взам. инв. №

Подпись и дата

Инв. № подл.

1852-СЗИ

					1852-СЗИ				
Изм	Лист	№ докум.	Подпись	Дата					
Разраб.		С.В. Городилов		27.10.17	Пояснительная записка		Лит.	Лист	Листов
Пров.		С.В. Городилов		27.10.17			ТП	1	
							ООО ТК «АСПЕКТ-СЕТИ»		
Н.контр.		К.В. Редкин		27.10.17					
				27.10.17					

1. Общие положения

Предметом настоящего документа является разработка требований и решений по системе защиты персональных данных, обрабатываемых в системе управления и контроля доступом (СКУД) в здания Кировского регионального отделения Фонда социального страхования Российской Федерации.

Адрес объекта: г. Киров, ул. Дерендяева, 77.

Заказчик: Кировское региональное отделение Фонда социального страхования Российской Федерации.

Система защиты персональных данных СКУД проектируется совместно с СКУД на основании государственного контракта № 15/384 от «28» августа 2017. г.

2. Нормативно-правовые основания

Система защиты информации СКУД разрабатывается на основании
следующих законов и нормативных документов:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 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».

Взам. инв. №	Подп. и дата	<p>обработке в информационных системах персональных данных»;</p> <p>– 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».</p>					Лист							
								Инв. № подл.	1852-СЗИ					2
Изм.	Лист	№ докум.	Подпись	Дата										

3. Используемые сокращения

АРМ – Автоматизированное рабочее место

БД – база данных

ИСПДн – информационная система персональных данных

ОС – операционная система

ПДн – персональные данные

СКУД – система контроля и управления доступом

ФСТЭК – Федеральная служба по техническому и экспортному контролю

4. Технологические процессы обработки информации

СКУД реализована на базе решения разработки компании Болид. В составе решения используются АРМ «Орион Про», контроллеры, пульта и конверторы серии С2000.

Сведения о СКУД, размещении оборудования и кабельных линий приведены в документе «Административные здания по адресу: г. Киров, ул. Дерендяева, 77. Система контроля и управления доступом. Рабочая документация», шифр 1852-СКУД.

Общая схема подключения основных узлов системы приведена на рисунке 2.

Инв. № подл	Подп. и дата	Взам. инв. №					
Изм.	Лист	№ докум.	Подпись	Дата	1852-СЗИ		Лист
							3

Классификация ИСПДн СКУД производится на основании следующих данных:

1. Категории персональных данных, обрабатываемых в ИСПДн СКУД: **иные.**
2. Объем обрабатываемых персональных данных: **до 100 000.**
3. Угрозы, актуальные для ИСПДн СКУД: **угрозы 3-го типа** (для информационной системы актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе).
4. Тип субъектов персональных данных, обрабатываемых в ИСПДн СКУД: **обрабатываются персональные данные субъектов персональных данных, являющихся сотрудниками оператора.**

На основании полученных данных, согласно Постановлению правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» информационной системе персональных данных ИСПДн СКУД следует обеспечивать **4-й уровень защищенности персональных данных (УЗ4).**

6. Оценка угроз безопасности информации

Оценка и составление перечня актуальных угроз безопасности персональных данных производится на основании методических документов ФСТЭК и с учетом банка данных угроз ФСТЭК:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008, утверждена заместителем директора ФСТЭК России;
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

Инв. № подл	Подп. и дата	Взам. инв. №	Оценка и составление перечня актуальных угроз безопасности персональных данных производится на основании методических документов ФСТЭК и с учетом банка данных угроз ФСТЭК:									
			1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008, утверждена заместителем директора ФСТЭК России;									
			2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах									
Изм.	Лист	№ докум.	Подпись	Дата	1852-СЗИ					Лист		
										6		

персональных данных от 14.02.2008, утверждена заместителем директора ФСТЭК России;

6.1. Уровень исходной защищенности по модели

Под уровнем исходной защищенности компонента У1 ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ресурса.

По каждой из основных 7-ми характеристик компонента определяется уровень исходной защищенности в соответствии с правилом:

Таблица 1 – определение исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
– распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	Н
– городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	Н
– корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	С	–
– локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	С	–
– локальная ИСПДн, развернутая в пределах одного здания	В	–	–
2. По наличию соединения с сетями общего пользования:			
– ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	Н
– ИСПДн, имеющая односточечный выход в сеть общего пользования;	–	С	–
– ИСПДн, физически отделенная от сети общего пользования	В	–	–
3. По встроенным (легальным) операциям с			

Инов. № подл	Подп. и дата	Взам. инв. №

Изм.	Лист	№ докум.	Подпись	Дата	1852-СЗИ	Лист
						7

Инов. № подл	Подп. и дата	Взам. инв. №

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
записями баз персональных данных:			
– чтение, поиск;	В	–	–
– запись, удаление, сортировка;	–	С	–
– модификация, передача	–	–	Н
4. По разграничению доступа к персональным данным:			
– ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	С	–
– ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	Н
– ИСПДн с открытым доступом	–	–	Н
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
– интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	Н
– ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	В	–	–
6. По уровню обобщения (обезличивания) ПДн:			
– ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	В	–	–

3. Присваивается **низкий уровень** ($Y1 = 10$) исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Исходя из оценок, данных выше в таблице 1, исходный уровень защищенности ИСПДн СКУД – **средний**.

4.2. Выбор актуальных типов нарушителя

Согласно «Базовой модели угроз ...» [2] источниками угроз безопасности, реализуемых за счет НСД, являются:

- нарушитель – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации;
- носитель вредоносной программы;
- аппаратная закладка.

Последние два источника реализации угроз связаны с действиями нарушителя и зависят от его возможностей, поэтому они рассматриваются в едином аспекте с первым источником.

Нарушители по наличию права постоянного или разового доступа к ресурсу подразделяются на внешних и внутренних.

Первая группа нарушителей реализует угрозы безопасности извне системы. К ней могут относиться: разведывательные службы государств, криминальные структуры, конкуренты (конкурирующие организации), недобросовестные партнеры, внешние субъекты (физические лица).

Нарушители второй группы, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализуют угрозы непосредственно в системе. Они подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к информации: К1 – должностные лица, обеспечивающие нормальное функционирование ИСПДн, К2 – зарегистрированные локальные пользователи ИСПДн, К3 –

Инв. № подл	Подп. и дата	Взам. инв. №	недобросовестные партнеры, внешние субъекты (физические лица).									
			Нарушители второй группы, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализуют угрозы непосредственно в системе. Они подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к информации: К1 – должностные лица, обеспечивающие нормальное функционирование ИСПДн, К2 – зарегистрированные локальные пользователи ИСПДн, К3 –									
Изм.	Лист	№ докум.	Подпись	Дата	1852-СЗИ						Лист	
											10	

зарегистрированные удаленные пользователи ИСПДн, К4 – зарегистрированные пользователи с полномочиями Администратора безопасности сегмента (фрагмента) ИСПДн, К5 – зарегистрированные пользователи с полномочиями Системного администратора ИСПДн, К6 – зарегистрированные пользователи с полномочиями Администратора безопасности ИСПДн, К7 – программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте, К8 – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Актуальные категории нарушителей определяются путем экспертной оценки. Экспертная оценка проводится путем присвоения каждому типу нарушителя вербального значения: н – низкая актуальность, с – средняя актуальность, в – высокая актуальность. Общая оценка по большинству одинаковых оценок.

Данные экспертной оценки представлены в документе «Оценка угроз информационной безопасности» в Таблице № 2 – Выбор актуальных типов нарушителя.

Таблица 2 – выбор актуальных типов нарушителя

Иденти- фикаторы	Категории нарушителей	Экспертная оценка опасности угроз			
		Эксперт1	Эксперт2	Эксперт3	Общая оценка
Внутренние нарушители					
К1	Должностные лица, обеспечивающие нормальное функционирование АС	с	с	с	Средняя
К2	Зарегистрированные локальные пользователи АС	с	с	с	Средняя
К3	Зарегистрированные удаленные пользователи АС	н	н	н	Низкая
К4	Зарегистрированные	н	н	н	Низкая

Изм.	Лист	№ докум.	Подпись	Дата	1852-СЗИ	Лист
						11

Инв. № подл	Подп. и дата	Взам. инв. №	

	пользователи с полномочиями Администратора безопасности сегмента (фрагмента) АС				
K5	Зарегистрированные пользователи с полномочиями Системного администратора АС	В	В	В	Высокая
K6	Зарегистрированные пользователи с полномочиями Администратора безопасности АС	В	В	В	Высокая
K7	Программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте	С	С	С	Средняя
K8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АС	С	С	С	Средняя
Внешние нарушители					
K9	Разведывательные службы государств	Н	Н	Н	Низкая
K10	Криминальные структуры (хакеры, группы хакеров)	В	В	В	Высокая
K11	Конкуренты (конкурирующие организации)	Н	Н	Н	Низкая
K12	Недобросовестные партнеры	Н	Н	Н	Низкая
K13	Внешние субъекты (физические лица)	Н	Н	Н	Низкая

4.2. Определение актуальных угроз безопасности

Определение актуальных угроз выполняется с учетом представлений об уязвимостях в соответствующих сегментах РИС.

Из выбранного ранее базового перечня угроз выбираются те, которые относятся к актуальным в соответствии с правилом, приведенным в таблице 3.

Таблица 3 – определение актуальности угрозы

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Определение актуальности угроз представлено в документе «Оценка угроз информационной безопасности» в Таблице 4 – Определение актуальных угроз безопасности по модели ФСТЭК, столбец 12.

7. Выбор мероприятий по обеспечению безопасности ПДн

Перечень мер защиты информации производится согласно Приказу ФСТЭК от 18.02.2013 №21 и приведен в Приложении Б.

Перечень мер, нейтрализующих угрозы информационной безопасности, определенные в модели угроз безопасности персональных данных приведен в Приложении В.

Основные технические решения, применяемые в ЛВС следующие:

- локальная сеть ИСПДн СКУД выполняется в изолированном от других сетей виде.
- в качестве операционных систем ПК и сервера применяются ОС Windows 10 Professional с усиленными настройками ограничения доступа, разделением полномочий администратора и пользователя.
- в качестве средства защиты от несанкционированного доступа и контроля машинных носителей информации применяется Dallas Lock 8-K;
- в качестве средства доверенной загрузки АРМ и сервера применяется средство доверенной загрузки Dallas Lock;
- в качестве электронных идентификаторов для доверенного запуска системы и входа в операционную систему применяются идентификаторы Рутокен 32К, сертифицированные ФСТЭК;
- в качестве антивирусного решения и решения по защите от типовых атак применяется Kaspersky Endpoint Security 10.

При внедрении СЗИ требуется разработать и принять следующие документы:

- приказ о внедрении системы защиты информации ИСПДн СКУД и назначении ответственных лиц;
- руководство пользователя;
- руководство администратора;
- инструкция по эксплуатации;

Приложение А – определение актуальных угроз

Таблица А.1 – определение актуальных угроз безопасности по модели ФСТЭК

		Экспертная оценка частоты (вероятности) реализации угроз					Экспертная оценка опасности угроз				
1	2	3	4	5	6	7	8	9	10	11	12
Иденти- фикаторы	Базовый перечень	Эксперт1	Эксперт2	Эксперт3	Общая оценка	КР	Эксперт1	Эксперт2	Эксперт3	Общая оценка	АУ
a	+	1	0	0	0	0,27	н	н	н	Низкая	Неактуальная
b	+	9	9	9	9	0,70	с	с	с	Средняя	Актуальная
c	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
d											
d1	+	2	2	2	2	0,35	с	н	н	Низкая	Неактуальная
d2	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
d3	+	5	5	5	5	0,50	с	с	с	Средняя	Актуальная
e											
e1	+	2	2	2	2	0,35	н	н	с	Низкая	Неактуальная
e2	+	2	2	2	2	0,35	н	н	с	Низкая	Неактуальная
f											
f1	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
f2	+	10	10	10	10	0,75	в	в	с	Высокая	Актуальная
f3	+	3	2	2	2	0,37	с	с	с	Средняя	Актуальная
f4	+	0	0	0	0	0,25	н	н	с	Низкая	Неактуальная
f5	+	0	0	0	0	0,25	н	н	с	Низкая	Неактуальная
f6	+	5	5	5	5	0,50	с	с	с	Средняя	Актуальная
f7	+	3	3	3	3	0,40	с	с	с	Средняя	Актуальная
g											
g1		0	0	0			в	в	с	Высокая	
g2	+	10	10	10	10	0,75	н	с	с	Средняя	Актуальная
g3	+	4	4	4	4	0,45	с	с	с	Средняя	Актуальная
g4	+	3	3	3	3	0,40	в	в	в	Высокая	Актуальная

Взам. инв. №	
Подл. и дата	
Инв. № подл	

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ

g5	+	1	1	1	1	0,30	в	в	в	Высокая	Актуальная
g6	+	5	5	5	5	0,50	с	с	в	Средняя	Актуальная
g7	+	10	10	9	10	0,73	в	с	в	Высокая	Актуальная
g8	+	7	7	7	7	0,60	с	с	с	Средняя	Актуальная
g9	+	10	10	10	10	0,75	в	в	в	Высокая	Актуальная
h											
h1	+	2	2	2	2	0,35	н	с	с	Средняя	Актуальная
h2	+	2	2	2	2	0,35	с	с	с	Средняя	Актуальная
h3	+	3	3	3	3	0,40	с	с	с	Средняя	Актуальная
h4	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
h5	+	5	5	5	5	0,50	н	н	с	Низкая	Неактуальная
h6	+	2	2	2	2	0,35	н	н	с	Низкая	Неактуальная
i											
i1	+	2	2	2	2	0,35	н	н	с	Низкая	Неактуальная
i2	+	5	5	5	5	0,50	н	с	с	Средняя	Актуальная
i3	+	5	5	5	5	0,50	с	с	с	Средняя	Актуальная
i4	+	5	5	5	5	0,50	с	с	с	Средняя	Актуальная
i5	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
i6	+	5	5	5	5	0,50	н	с	с	Средняя	Актуальная
i7	+	5	5	5	5	0,50	с	с	н	Средняя	Актуальная
i8	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
i9	+	0	0	0	0	0,25	н	н	н	Низкая	Неактуальная
i10	+	2	2	2	2	0,35	н	н	н	Низкая	Неактуальная

Таблица А.2 – общий перечень угроз и актуальные угрозы

ИД	Наименование угрозы	АРМ
a	Угрозы утечки акустической (речевой) информации:	Неактуальная
b	Угрозы утечки видовой информации	Актуальная

Взам. инв. №	
Подп. и дата	
Инв. № подл	

c	Угрозы утечки информации по каналу ПЭМИН	Неактуальная
d	Угрозы, реализуемые в ходе загрузки ОС и направленные на:	
d1	перехват паролей или идентификаторов	Неактуальная
d2	модификация базовой системы ввода/вывода (BIOS)	Неактуальная
d3	перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в ОС ИС	Актуальная
e	Преднамеренные действия внутренних нарушителей	
e1	Доступ к информации, ее модификация и уничтожение лицами, не допущенными к обработке	Неактуальная
e2	Разглашение информации, ее модификация и уничтожение сотрудниками, допущенными к обработке	Неактуальная
f	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно аппаратных и программных средств (в том числе программно математических воздействий)	
f1	внедрение злонамеренных программных закладок	Неактуальная
f2	внедрение вирусов	Актуальная
f3	внедрение других вредоносных программ, предназначенных для осуществления НСД (ПО подбора паролей, ПО реализующие известные уязвимости, ПО для генерации вирусов и т.п.)	Актуальная
f4	Недекларированные возможности в прикладном ПО	Неактуальная
f5	Недекларированные возможности в системном ПО	Неактуальная
f6	Установка ПО, не требующегося для исполнения служебных обязанностей	Актуальная
f7	НСД с использованием мобильного кода (javascript, pdf, flash, html5 и т.п.)	Актуальная
g	Угрозы, реализуемые при сетевом и межсетевом взаимодействии ПК	
g1	«Анализ сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	
g2	Угрозы сканирования, направленные на выявление типа ОС ИС, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.	Неактуальная
g3	Внедрение ложного объекта	Актуальная
g4	Навязывание ложного маршрута	Актуальная
g5	Подмена доверенного объекта	Актуальная
g6	Выявления паролей по сети	Неактуальная
g7	«Отказ в обслуживании»	Актуальная
g8	Удаленный запуск приложений	Неактуальная
g9	Внедрение по сети вредоносных программ	Актуальная
h	Угрозы уничтожения, хищения аппаратных средств ИС путем физического доступа к элементам ИС	

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ

Лист

20

h1	Кража элементов, содержащих обрабатываемую в ИС информацию (носителей информации)	Актуальная
h2	Кража ключей и атрибутов доступа	Актуальная
h3	Кража, уничтожение, модификация информации	Актуальная
h4	Вывод из строя узлов ПЭВМ и каналов связи	Неактуальная
h5	Несанкционированный доступ к информации при техническом обслуживании узлов ИС	Неактуальная
h6	Несанкционированное отключение средств защиты информации	Неактуальная
i	Непреднамеренные действия пользователей, нарушения безопасности функционирования СЗИ, а также угрозы неантропогенного и стихийного характера	
i1	Утрата или несоблюдение порядка действий с ключами и атрибутами доступа	Неактуальная
i2	Непреднамеренная модификация (уничтожение) информации сотрудниками	Актуальная
i3	Некомпетентные действия администратора	Актуальная
i4	Непреднамеренное отключение средств защиты	Актуальная
i5	Выход из строя аппаратных и программных средств	Актуальная
i6	Нарушения условий обслуживания, включая несанкционированную передачу носителей информации	Актуальная
i7	Сбой системы электроснабжения	Актуальная
i8	Сбой системы охлаждения	Неактуальная
i9	Затопление серверной	Неактуальная
i10	Стихийное бедствие	Неактуальная

Взам. инв. №	
Подп. и дата	
Инв. № подл	

Изм.	Лист	№ докум.	Подпись	Дата

				Лист
1852-СЗИ				21

Приложение Б – выбор мер информационной безопасности

Таблица Б.1 - Перечень мер информационной безопасности

Усл. обозн. и номер меры	Меры защиты информации в информационных системах	Базовый набор мер	Адаптация	Уточнение (по модели угроз)	Описание реализации меры и усиление для соответствующего класса
					УЗ-4 (СКУД)
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+			Средства аутентификации Dallas Lock 8-K
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			g3, g4, g5	Компенсирующие меры – ограничение доступа в помещения, стационарная эксплуатация оборудования, контроль подключения к коммутатору и портам СКС оборудования.
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+		h2	Средства аутентификации Dallas Lock 8-K
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	+		h2	Политики в Windows, сложные пароли длиной не менее 6 символов и применение 3 групп символов.

Изм. инв. №	
Подп. и дата	
Инв. № подл	

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		22

Изм. № подл	Подп. и дата	Взам. инв. №

ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+			Скрытие пароля при входе в Windows
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+			Неактуально.
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа				Не требуется
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	+			Средства Dallas Lock 8-K
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+		i2	Предусматривается ролевая и дискреционная модели разграничения доступа: Dallas Lock 8-K, Windows. Разграничение доступа выполняется системным администратором на основании допуска пользователей и полномочий.
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача	+	ИСКЛ		Ограничение потоков путем ограничения функционала АРМ и сервера.

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ

Лист

23

Взам. инв. №	
Подп. и дата	
Инв. № подл	

	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	+		i2	Выполняется во всех уровнях реализации с использованием Dallas Lock 8-K, Windows
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+		i2	Предусмотрено в Windows, Dallas Lock 8-K
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+		h2	Предусмотрено в Windows, Dallas Lock 8-K
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации				Не требуется
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				Не требуется
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				Не требуется

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		24

Изм. № подл	Подп. и дата	Взам. инв. №

УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу			b el	Предусмотрено в Windows, Dallas Lock 8-K Усиление: 1б) блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя в течение 15 минут;
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации				Не требуется
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				Не требуется
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+		g2-g5, g9	Не актуально. Сеть СКУД изолирована.
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	ИСКЛ		Не характерно для системы.
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	ИСКЛ		Не характерно для системы.
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	ИСКЛ		Не актуально. Сеть СКУД изолирована.

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		25

Взам. инв. №	
Подп. и дата	
Инв. № подл	

УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			d3 h2	Средство доверенной загрузки Dallas Lock, опечатывание корпуса, ограничение доступа в помещения, стационарная эксплуатация оборудования, ответственные лица.
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				Не требуется
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				Не требуется
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов			f6 i3	Организационные меры – периодический контроль системным администратором.
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				Не требуется
IV. Защита машинных носителей информации (ЗНИ)					
ЗНИ.1	Учет машинных носителей информации	+		h1	Ведение журнала учета МНИ.

					1852-СЗИ	Лист
						26
Изм.	Лист	№ докум.	Подпись	Дата		

Изм. № подл	Подп. и дата	Взам. инв. №

					Выдача МНИ под роспись. Выборочный запрет на использование МНИ. Ограничение МНИ в Dallas Lock 8-К.
ЗНИ.2	Управление доступом к машинным носителям информации				Не требуется
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				Не требуется
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах				Не требуется
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации				Не требуется.
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации				Не требуется
ЗНИ.7	Контроль подключения машинных носителей информации				Не требуется
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль			i6	Организационные меры – согласование обслуживания и передачи носителей с ответственным за ИБ. Ответственность сотрудников.

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		27

Изм. № подл	Подп. и дата	Взам. инв. №

	уничтожения (стирания)				Техническая реализация: DallasLock 8-К.
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+			Определяется настройками по умолчанию Windows, Dallas Lock 8-К
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+			Определяется настройками по умолчанию Windows, DallasLock 8-К.
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	+		i2 i3	Не менее 6 месяцев. Определяется настройками Windows, DallasLock 8-К .
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				Не требуется
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них				Не требуется
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				Не требуется
РСБ.7	Защита информации о событиях безопасности	+			Реализуется по умолчанию в защищенные каталоги Windows.

					1852-СЗИ	Лист
						28
Изм.	Лист	№ докум.	Подпись	Дата		

Взам. инв. №	
Подп. и дата	
Инв. № подл	

VI. Антивирусная защита (AB3)					
AB3.1	Реализация антивирусной защиты	+		f2	Техническая реализация: Kaspersky Endpoint Security 10. Организационно – инструкция по безопасной обработке ПДн.
AB3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+			Техническая реализация: Kaspersky Endpoint Security 10. Организационно – инструкция по безопасной обработке ПДн.
VII. Обнаружение вторжений (COB)					
COB.1	Обнаружение вторжений			g2, g9	Техническая реализация: Kaspersky Endpoint Security 10.
COB.2	Обновление базы решающих правил				Техническая реализация: Kaspersky Endpoint Security 10.
VIII. Контроль (анализ) защищенности информации (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей			g2, g9	Мониторинг администратором информации на сайтах и рассылках производителей и независимых источников. Реализация: Windows Update, обновление сторонних программ администратором.
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного	+		g2, g9	Периодический контроль и выполнения администратором вручную, тестирование

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ

Взам. инв. №	
Подп. и дата	
Инв. № подл	

	обеспечения средств защиты информации				обновлений. Windows Update.
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации			g2, g9	Периодический контроль работоспособности администратором ИБ, тестирование ПО перед установкой на рабочую систему.
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации			g2, g9	Организационные меры – ежедневный и периодический мониторинг, принятие мер при несанкционированных изменениях в составе ПО и оборудования.
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе			g2, g9	Контроль системным администратором.
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			f6	Контроль системным администратором.
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы			i2	Контроль специалистом по СКУД, операторами СКУД.
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное			i2 i5	Восстановление обеспечивается наличием дистрибутивов ПО на месте, резервных

					1852-СЗИ	Лист
						30
Изм.	Лист	№ докум.	Подпись	Дата		

Изм. № подл	Подп. и дата	Взам. инв. №

	обеспечение средств защиты информации, при возникновении нештатных ситуаций				копий базы данных
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)				Не требуется
ОЦЛ.5	Контроль содержания информации, передаваемой из ИС (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из ИС				Не требуется
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему			i2	Должно обеспечиваться на уровне прикладного ПО и прав доступа к функционалу ПО, Ответственность пользователей
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему			i2	Должно обеспечиваться на уровне прикладного ПО, Ответственность пользователей
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			i2	Должно обеспечиваться на уровне прикладного ПО, Ответственность пользователей

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		31

Х. Обеспечение доступности информации (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				Не требуется
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				Не требуется
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	+			Не требуется
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации			i2 i5	Ежедневная резервная копия базы данных СКУД в перерыве на обед и после работы.
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала			i2 i5	Ежедневная резервная копия базы данных СКУД в перерыве на обед и после работы.
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	+	ИСКЛ		Неприменимо.
ЗСВ.2	Управление доступом субъектов доступа к	+	ИСКЛ		Неприменимо.

Изм. № подл	Подп. и дата	Взам. инв. №

	объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин				
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		ИСКЛ		Неприменимо.
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры		ИСКЛ		Неприменимо.
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией		ИСКЛ		Неприменимо.
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		ИСКЛ		Неприменимо.
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		ИСКЛ		Неприменимо.
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры		ИСКЛ		Неприменимо.
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	ИСКЛ		Неприменимо.
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации		ИСКЛ		Неприменимо.

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		33

Изм. № подл	Подп. и дата	Взам. инв. №

	отдельным пользователем и (или) группой пользователей				
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				Не актуально
ЗТС.2	Организация контролируемой зоны (КЗ), в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования			h1	Не актуально
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, исключаящие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+		h1	Перечень допущенных и ответственных за помещения лиц определяется приказом. Учет физического доступа ведется: - учет выдачи ключей; - учет доступа в СКУД.
ЗТС.4	Размещение устройств вывода (отображения) информации, исключаяющее ее несанкционированный просмотр	+		b	Должно обеспечиваться организационно

Изм. № подл	Подп. и дата	Взам. инв. №

ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)			i7 i8	ИБП для сервера и АРМ.
ХIII. 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 информации, функций по обработке информации и иных функций информационной системы				Должно быть реализовано в DallasLock 8-K, Windows, СКУД
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				Не требуется
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	ИСКЛ		Не характерно
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				Не требуется
ЗИС.5	Запрет несанкционированной удаленной	+	ИСКЛ		Неприменимо

Изм. № подл	Подп. и дата	Взам. инв. №

	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 информацией, при обмене информацией с иными информационными системами				Не требуется
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				Не требуется
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				Не требуется
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеoinформации, в том числе регистрация событий, связанных с передачей видеoinформации, их анализ и реагирование на нарушения, связанные с				Не требуется

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ	Лист
	36

Изм. № подл.	Подп. и дата	Взам. инв. №

	передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				Не требуется
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов				Не требуется
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю				Не требуется
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя				Не требуется
ЗИС.14	Использование устройств терминального доступа для обработки информации				Не требуется
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации				Не требуется
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов				Не требуется

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		37

Инв. № подл	Подп. и дата	Взам. инв. №

ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы				Не требуется
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения				Не требуется
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				Не требуется
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе				Неприменимо.
XIII. 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				Администратор и обслуживающие лица определяются приказом и договорами
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных				В функциях администратора системы
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и				Функция Администратора и лица, обслуживающего СКУД.

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		38

Инов. № подл	Подл. и дата	Взам. инв. №

	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				В функциях администратора системы

Приложение В – Перечень актуальных угроз и нейтрализующих мер

Таблица В.1 - Перечень актуальных угроз и нейтрализующих их мер

ИД	Наименование угрозы	Сегмент	Мера согласно Приказу 21 ФСТЭК	Организационные меры	Особенности
		СКУД			
b	Угрозы утечки видовой информации	Да	ЗТС.4, УПД.10	Требования в инструкции по безопасной обработке ПДн	
d	Угрозы, реализуемые в ходе загрузки ОС и направленные на:				
d3	<ul style="list-style-type: none"> перехват управления с изменением необходимой технологической информации для получения НСД в ОС ИС 	Да	УПД.17	Ограничение доступа в помещения, Исключение необнаруживаемого доступа (опечатывание помещений), Ответственность работников	АРМ Операторов: опечатывание корпуса ПК, ограничение порядка загрузки, пароль BIOS.
f	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением				

Изм. № подл.	Подп. и дата	Взам. инв. №

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ

Изм. № подл	Подп. и дата	Взам. инв. №

	программно аппаратных и программных средств (в том числе программно математических воздействий)				
f2	<ul style="list-style-type: none"> внедрение вирусов 	Да	АВЗ	Требования к антивирусному контролю в инструкции по безопасной обработке ПДн	
f3	<ul style="list-style-type: none"> внедрение других вредоносных программ, предназначенных для осуществления НСД (ПО подбора паролей, ПО реализующие известные уязвимости, ПО для генерации вирусов и т.п.) 	Да	АВЗ	Требования к антивирусному контролю в инструкции по безопасной обработке ПДн	Ограничение с помощью средств контроля и запуска приложений KES
f6	<ul style="list-style-type: none"> Установка ПО, не требующегося для исполнения служебных обязанностей 	Да	АВЗ, ОПС.2, ОЦЛ.1	Требования к антивирусному контролю в инструкции по безопасной обработке ПДн	Ограничение с помощью средств контроля и запуска приложений KES
	<ul style="list-style-type: none"> НСД с использованием мобильного кода (javascript, pdf, flash, html5 и т.п.) 	Да	АВЗ, ОПС.2	Требования к антивирусному контролю в инструкции по безопасной обработке ПДн	

Изм.	Лист	№ докум.	Подпись	Дата

1852-СЗИ

Взам. инв. №	
Подл. и дата	
Инв. № подл	

g	Угрозы, реализуемые при межсетевом взаимодействии				
g2	<ul style="list-style-type: none"> Угрозы сканирования, направленные на выявление типа ОС ИС, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др. 	Да	УПД.13, СОВ.1, АНЗ	Межсетевой экран	Механизмы обнаружения и блокировки атак KES
g3	<ul style="list-style-type: none"> Внедрение ложного объекта 	Да	УПД.13, ИАФ.2, ЗИС.3, ЗИС.11		Механизмы обнаружения и блокировки атак KES
g4	<ul style="list-style-type: none"> Навязывание ложного маршрута 	Да	УПД.13, ИАФ.2, ЗИС.3, ЗИС.11		Механизмы обнаружения и блокировки атак KES
g5	<ul style="list-style-type: none"> Подмена доверенного объекта 	Да	УПД.13, ИАФ.2, ЗИС.3, ЗИС.11	Режимные меры на объектах	Механизмы обнаружения и блокировки атак KES
g9	<ul style="list-style-type: none"> Внедрение по сети вредоносных программ 	Да	УПД.13, АВЗ, СОВ, АНЗ	Регламентация мер антивирусной защиты, защиты от атак	Применение KES
h	Угрозы уничтожения, хищения аппаратных средств ИС путем				

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		42

Взам. инв. №	
Подп. и дата	
Инв. № подл	

	физического доступа к элементам ИС				
h1	<ul style="list-style-type: none"> Кража элементов, содержащих обрабатываемую в ИС информацию (носителей информации) 	Да	ЗНИ.1, ЗТС.2-3	Инструкция по порядку учёта, хранения и уничтожения носителей персональных данных, Оперативное отключение узла при инциденте, Расследование инцидента	
h2	<ul style="list-style-type: none"> Кража ключей и атрибутов доступа 	Да	УПД.17, ИАФ.3, ИАФ.4, УПД.6	Перечень ответственных лиц, Ограничение доступа в помещения, Исключение необнаруживаемого доступа (опечатывание, сигнализация), Учет ключей доступа, Ответственность, Обучение пользователей, Оперативное отключение узла при инциденте, Расследование инцидента	
h3	<ul style="list-style-type: none"> Кража, уничтожение, модификация информации 	Да	ИАФ, УПД, РСБ, ЗНИ	Перечень ответственных лиц, Ограничение доступа в помещения, Исключение необнаруживаемого доступа, Учет ключей доступа, Ответственность, Обучение пользователей, Оперативное отключение узла при обнаружении кражи, Расследование инцидента	
i	Непреднамеренные действия пользователей, нарушения функционирования СЗИ, а также угрозы неантропогенного и стихийного характера				

Изм.	Лист	№ докум.	Подпись	Дата

Изм. № подл	Подп. и дата	Взам. инв. №

i1	<ul style="list-style-type: none"> Утрата или несоблюдение порядка действий с ключами и атрибутами доступа 	Да		Перечень ответственных лиц, Ограничение доступа в помещения, Исключение необнаруживаемого доступа, Учет ключей доступа, Ответственность, Обучение пользователей	
i2	<ul style="list-style-type: none"> Непреднамеренная модификация (уничтожение) информации сотрудниками 	Да	УПД.2, УПД.4, УПД.5, ОЦЛ.3, РСБ.3, ОЦЛ.6-8, ОДТ.4-5	Регламентация порядка выполнения резервных копий, Назначение ответственного лица, Выполнение резервного копирования, Ответственность пользователей	Резервное копирование СКУД, контроль сотрудниками информации в ИС
i3	<ul style="list-style-type: none"> Некомпетентные действия администратора 	Да	ОПС.2, ОПС.3, РСБ.3, УКФ.3	Обучение, Техническая поддержка и сопровождение компетентным подрядчиком (по договору)	
i4	<ul style="list-style-type: none"> Непреднамеренное отключение средств защиты 	Да	УПД.2, УПД.4, УПД.5, ОЦЛ.3	Обучение, Техническая поддержка и сопровождение компетентным подрядчиком (по договору)	
i5	<ul style="list-style-type: none"> Выход из строя аппаратных и программных средств 	Да	ОДТ.1, ОЦЛ.3, ОДТ.4	Регламентация профилактического обслуживания и его регулярное проведение, Ежедневный контроль состояния оборудования, Своевременная замена оборудования	Ежедневные резервные копии данных для восстановления не более 24 часов
i6	<ul style="list-style-type: none"> Нарушения условий обслуживания, включая 	Да	ЗНИ.8	Соблюдение инструкции по безопасной обработке ПДн	

Инов. № подл	Подл. и дата	Взам. инв. №

	несанкционированную передачу носителей информации				
i7	<ul style="list-style-type: none"> Сбой системы электроснабжения 	Да	ЗТС.5	Организационные меры. Контроль ИБП	

					1852-СЗИ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		45