МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.03 —	Информационная безопасность автоматизированных систем
Специализация — 6	Защищенные автоматизированные системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В АО «ФНПЦ «ПО «СТАРТ» ИМ. М.В. ПРОЦЕНКО»

Студент	_____	Коваленко Ольга Сергеевна
Руководитель	_____	Мартынов Александр Евгеньевич
Нормоконтролёр	_____	Фатеев Алексей Григорьевич
Рецензент инженер по защите информации АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»	_____	Шпагин Денис Юрьевич

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой _____ С.Л.Зефиров

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 26.06.20 № 12)

Секретарь ГЭК _____ А.П. Иванов

Пенза 2020

Оглавление

Введение.....5
1 Описание субъекта критической информационной инфраструктуры.....8
2 Определение объектов критической информационной инфраструктуры.....11
2.1 Создание комиссии по категорированию объектов критической информационной инфраструктуры.....11
2.2 Порядок определения объектов критической информационной инфраструктуры.....11
2.3 Определение процессов субъекта критической информационной инфраструктуры и выявление среди них критических 12
2.4 Определение объектов критической информационной инфраструктуры, необходимых для критических процессов.....21
3 Методика проведения категорирования типовых автоматизированных систем в защищенном исполнении и основных информационных систем.....22
4 Создание системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры.....29
5 Установка требований, которые необходимо выполнить для обеспечения безопасности каждого значимого объекта критической информационной инфраструктуры и формирование плана мероприятий.....33
6 Моделирование угроз безопасности информации на значимых объектах критической информационной инфраструктуры.....36
6.1 Моделирование угроз безопасности. Общие положения.....36
6.2 Модель нарушителя.....36
6.3 Определение актуальности угроз безопасности информации.....43
6.4 Описание актуальных угроз безопасности информации.....111
7 Внедрение организационных и технических мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры..... ….....117

7.1 Базовый набор мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры.....117
7.2 Техническое задание на создание системы безопасности значимого объекта.....117
8 Описание взаимодействия субъекта критической информационной инфраструктуры с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.....125
9 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....131
Заключение.....133
Список использованных источников.....134
Приложение А Приказ о создании комиссии по категорированию.....136
Приложение Б Перечень объектов критической информационной инфраструктуры 139
Приложение В Акт о результатах присвоения критическим процессам объекта критической информационной инфраструктуры категории значимости.....140
Приложение Г Акт о результатах присвоения объекту критической информационной инфраструктуры категории значимости 148
Приложение Д Приказ о создании системы безопасности значимых объектов критической информационной инфраструктуры ….....160
Приложение Е Приказ о назначении ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры.....161
Приложение Ж План проведения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры.....163
Приложение И Модель нарушителя.....164
Приложение К Модель угроз безопасности информации ….....171

Приложение Л Базовый набор мер по обеспечению безопасности значимого объекта для III категории значимости ….....264
Приложение М Техническое задание на создание системы безопасности значимого объекта критической информационной инфраструктуры.....270
Приложение Н Приказ об организации взаимодействия с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.....286

Введение

В настоящий момент большинство сфер жизни человека, общества и государства зависят от информационных инфраструктур. Исходя из этого вопрос информационной безопасности стал актуальным на международном уровне. В большинстве случаев кибер-атакам подвержены объекты критической информационной инфраструктуры, а именно: информационно-телекоммуникационные системы, информационные системы, автоматизированные системы управления государственных органов, учреждений и компаний, функционирующих во всех областях деятельности городов, субъектов, а так же всей страны в целом.

Субъектами критической информационной инфраструктуры являются организации и предприятия, которые работают в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и других сферах финансового рынка, топливно-энергетического комплекса, в областях атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Они обязаны выполнять требования по безопасности, установленные 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».[1]

Непрерывное, а так же устойчивое функционирование критической информационной инфраструктуры при проводимых по отношению к ней компьютерных атак — основное правило обеспечения информационной безопасности критической информационной инфраструктуры. Поскольку остановка какого-либо технологического процесса или бизнес процесса, следующая за отказом системы, вероятно приведет к потерям, которые измеряются не только денежным отношением, но и человеческими жизнями. Исходя из этого важно обеспечить высокий уровень надежности и отказоустойчивости системы безопасности значимых объектов критической информационной инфраструктуры.

Цель выпускной квалификационной работы — разработка проекта системы обеспечения безопасности объектов критической информационной инфраструктуры в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Задачи выпускной квалификационной работы:

– определение процессов субъекта критической информационной инфраструктуры (КИИ) и выявление среди них критических;

– определение объектов КИИ, необходимых для критических процессов;

– проведение категорирования значимого объекта КИИ;

– создание системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ);

– установка требований, которые необходимо выполнить для обеспечения безопасности каждого ЗОКИИ и формирование плана мероприятий;

– моделирование угроз безопасности информации на ЗОКИИ;

– внедрение организационных и технических мер по обеспечению безопасности ЗОКИИ;

– описание процесса взаимодействия субъекта КИИ с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА);

– изучение вредных психофизиологических факторов, влияющих на нервную систему специалиста по защите информации, так же методов и средств физической культуры, которые снижают их воздействие.

Актуальность создания системы безопасности значимых объектов критической информационной инфраструктуры на предприятии обусловлена необходимостью обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении по отношению к ней компьютерных атак.

1 января 2018 года вступил в силу Федеральный закон от 26.07.2017г. N187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».[1] Еще на этапе проекта, в 2013 году, этот закон начал активно обсуждаться и вызывать много вопросов касаемо практической реализации предъявляемых им требований. Сейчас, когда данные требования

стали действующими, и большинству организаций необходимо их выполнять, эти вопросы стали наиболее актуальными.

1 Описание субъекта критической информационной инфраструктуры

Субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей. [1]

Изначально необходимо определить, является ли АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» субъектом КИИ в рамках Федерального Закона №187 «О безопасности критической информационной инфраструктуры Российской Федерации». [1]

Для этого важно определить:

- является ли организация владельцем информационной системы;
- обеспечивает ли данная система надлежащую работу компании в одной из 13 критически важных сфер.

В Уставе АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» (Редакция от 15 октября 2018 года/Редакция №1), а именно в главе, посвященной основным видам деятельности предприятия, прямо упомянуты сферы деятельности, регулируемой по ФЗ-187. [1] Так же согласно Уставу организация является российским юридическим лицом. И в ведении данной организации есть информационные системы.

Часть видов деятельности предприятия по Уставу:

«4.2.3 Использование радиоактивных материалов при проведении работ

по использованию атомной энергии в оборонных целях.

4.2.4 Производство, научно-исследовательская и опытно-конструкторская работа, испытания, модернизация приборов автоматики оборонного назначения.

4.2.5 Производство, научно-исследовательская и опытно-конструкторская работа, испытания, модернизация, серийное сопровождение оборудования, приборов, аппаратуры, проведение ремонтных, монтажных и пусконаладочных работ для атомных электростанций и других объектов использования атомной энергии.»

«4.2.7 Разработка, производство и ремонт вооружения и военной техники.»

«4.2.12 Разработка, изготовление аппаратуры и компонентов, монтаж, наладка, ремонт и техническое обслуживание линий связи различного назначения, в том числе волоконно-оптических.»

«4.2.22 Эксплуатация электрических и тепловых сетей и обеспечение их работоспособности.»

«4.2.26 Монтаж, наладка, ремонт и техническое обслуживание средств телефонной связи и радиосвязи, предоставление услуг телефонной связи и трансляции звуковых программ по сети проводного вещания.»

«4.2.33 Перевозка пассажиров, народнохозяйственных и опасных грузов автомобильным транспортом.»

«4.2.37. Разработка, производство, реализация и ремонт технических систем и устройств, обеспечивающих безопасность движения на железных дорогах.»

«4.2.41. Выполнение государственного заказа по производству научно-технической продукции.»

На основе данных видов деятельности были выделены основные сферы деятельности предприятия по Уставу:

- топливно-энергетический комплекс;
- наука, транспорт, связь;

- военно промышленный комплекс;
- атомная промышленность.

Из этого можно сделать вывод, что АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» является субъектом КИИ в рамках ФЗ №187 «О безопасности критической информационной инфраструктуры Российской Федерации». [1]

2 Определение объектов критической информационной инфраструктуры

2.1 Создание комиссии по категорированию объектов критической информационной инфраструктуры

На первом этапе создается комиссия по категорированию объектов КИИ. В состав комиссии необходимо включить:

- генерального директора или уполномоченное им лицо;
- специалистов производства;
- специалистов промышленной безопасности;
- специалистов отдела АСУ ТП;
- специалистов отдела информационных технологий;
- ответственных за обеспечения безопасности в АСУ ТП;
- работников подразделения по защите государственной тайны;
- специалистов по промышленной безопасности, по гражданской обороне и защите от чрезвычайных ситуаций. [2]

Приказ о создании комиссии по категорированию представлен в приложении А.

Комиссия по категорированию подлежит расформированию, в случаях:

- прекращения субъектом КИИ выполнения функций (полномочий) или осуществления видов деятельности в областях (сферах);
- ликвидация, реорганизация субъекта КИИ и (или) изменения его организационно-правовой формы, в результате которых были утрачены признаки субъекта КИИ. [2]

2.2 Порядок определения объектов критической информационной инфраструктуры

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети,

автоматизированные системы управления субъектов критической информационной инфраструктуры. [1]

Для определения объектов КИИ необходимо:

- определить управленческие, технологические, производственные, финансово-экономические, а так же иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ;
- определить перечень критических процессов предприятия;
- определить ИС, ИТКС, АСУ, в которых:
- обрабатываемая информация является необходимой для обеспечения выполнения критических процессов;
- выполняется управление, контроль или мониторинг критических процессов;
- существуют угрозы безопасности информации;
- существуют уязвимости, которые могут привести к возникновению компьютерных инцидентов;
- потенциальный нарушитель, который может реализовывать свои возможности;
- составить перечень объектов КИИ. [2]

2.3 Определение процессов субъекта критической информационной инфраструктуры и выявление среди них критических

На следующем этапе необходимо выделить процессы предприятия (управленческие, технологические, финансово-экономические, производственные и так далее).

Были выделены следующие процессы:

- кадровая деятельность;
- вспомогательное производство;
- основное производство;

– ведение бухгалтерского учета;

– ведение налогового учета;

– закупочная деятельность.

Затем необходимо выделить среди данных процессов критические. Для этого используется перечень критериев значимости объектов и их значения из приложения 1 к Постановлению № 127. [3] Необходимо определить для каждого рассматриваемого процесса, может ли его нарушение повлечь последствия, определенные в Перечне.

Перечень критериев значимости объектов и их значения из приложения 1 к Постановлению № 127, [3] представлен в таблице 1.

Таблица 1 — Перечень критериев значимости объектов и их значения

Показатель	**Значение показателя**		
	III категория	II категория	I категория
I. Социальная значимость			
1 Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
2 Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта РФ или территории города федерального значения

Продолжение таблицы 1

	Показатель	Значение показателя		
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
4	Прекращение или нарушение функционирования сети связи, оцениваемые:			
	а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения

Продолжение таблицы 1

	Показатель	Значение показателя		
	б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее 6
	II. Политическая значимость			
6	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения	прекращение или нарушение функционирования федерального органа государственной власти	прекращение или нарушение функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации
7	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	нарушение условий договора межведомственного характера (срыв переговоров или подписания)	нарушение условий межправительственного договора (срыв переговоров или подписания)	нарушение условий межгосударственного договора (срыв переговоров или подписания)

Продолжение таблицы 1

	Показатель	Значение показателя		
	III. Экономическая значимость			
8	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
9	Возникновение ущерба бюджетам Российской Федерации, оцениваемого:			
	а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
	б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
	в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	более 0,01, но менее или равно 0,5	более 0,5, но менее или равно 1	более 1
10	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)	более 3, но менее или равно 70	более 70, но менее или равно 120	более 120

Продолжение таблицы 1

Показатель			Значение показателя	
IV. Экологическая значимость				
11. Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:				
	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;		выход за пределы территории одного муниципального образования или одной внутригородс-кой территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения	выход за пределы территории одного субъекта РФ или территории города федерального значения
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

Продолжение таблицы 1

Показатель		Значение показателя		
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта РФ и или города федерального значения	прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации	прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда РФ, Конституционного Суда РФ
13	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:			
	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
	б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	более 3, но менее или равно 10	более 10, но менее или равно 40	более 40
14	Прекращение или нарушение функционирования (невыполнения установленных показателей) ИС в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого ИС может быть недоступна пользователю (часов)	менее или равно 4, но более 2	менее или равно 2, но более 1	более 1

Нарушение процессов закупочной деятельности и ведения налогового учета, повлекут последствия экономической значимости.

Нарушение процессов вспомогательного и основного производства, повлекут последствия социальной и экологической значимости.

Нарушение процессов кадровой деятельности и ведение бухгалтерского учета, не повлекут последствий, определенных в Перечне.

Определение категории значимости критических процессов АО«ФНПЦ «ПО «Старт» им. М.В. Проценко» приведено в таблице 2.

Таблица 2 — Определение категории значимости критических процессов

№	Процесс	Показатель	Значение показателя	Категория значимости	Итоговая категория значимости
1	Закупочная деятельность	8.Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	более 5, но менее или равно 10	III категория	III категория
2	Ведение налогового учета	9.Возникновение ущерба бюджетам Российской Федерации, оцениваемого:			III категория
		а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	III категория	
		б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);	более 0,01, но менее или равно 0,5	III категория	

Продолжение таблицы 2

№	Процесс	Показатель	Значение показа-теля	Катего-рия значи-мости	Итоговая категория значи-мости
3	Основное произ-водство	1.Причинение ущерба жизни и здоровью людей (человек).	более или равно 1, но менее или равно 50	III категория	III категория
		11.Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:			
		а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	—	Без категории	
		б) по количеству людей, которые могут быть подвержены вредным воздействиям	—	Без категории	
4	Вспомога-тельное произ-водство	1.Причинение ущерба жизни и здоровью людей (человек).	более или равно 1, но менее или равно 50	III	III категория
		11.Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:			
		а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	—	Без категории	
		б) по количеству людей, которые могут быть подвержены вредным воздействиям	—	Без категории	

2.4 Определение объектов критической информационной инфраструктуры, необходимых для критических процессов

На следующем этапе для каждого критического процесса выделяются информационные системы (ИС), информационно телекоммуникационные системы (ИТКС), автоматизированные системы управления технологическим процессом (АСУ ТП), обрабатывающие информацию, которая необходима для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. Результат представлен в таблице 3.

Таблица 3 — Критические процессы

№	Критический процесс	ИС, ИТКС, АСУ ТП
1	Закупочная деятельность	Корпоративная сеть передачи данных
2	Ведение налогового учета	Система бухгалтерского учета
3	Основное производство	АСУ ТП основного производства
4	Вспомогательное производство	АСУ ТП вспомогательного производства

Затем, исходя из реального состава ИС, ИТКС и АСУ ТП, которые принадлежат субъекту КИИ на праве собственности, аренды или на другом законном основании, составляется перечень объектов КИИ, подлежащих категорированию.

Перечень объектов КИИ оформляется в соответствии с рекомендуемой ФСТЭК России формой, приведенной в Приложении 2, определенной Информационным сообщением ФСТЭК России «по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» от 24 августа 2018 г. № 240/25/3752. [4]

Перечень объектов КИИ представлен в приложении Б.

3 Методика проведения категорирования типовых автоматизированных систем в защищенном исполнении и основных информационных систем

В соответствии с Постановлением Правительства Российской Федерации от 8 февраля 2018 г. №127 (п. 14 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации) [3] комиссия по категорированию проводит оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объекте КИИ и присвоение каждому из объектов КИИ одной из категорий значимости либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости.

Оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объекте КИИ представлена в таблице 4.

Таблица 4 — Категория значимости объектов КИИ

№	Объект КИИ	Показатель	Значение показателя	Категория значимости	Итоговая категория значимости
1	Корпоративная сеть передачи данных	Возникновение ущерба субъекту КИИ, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом), стратегическим предприятием), оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший пятилетний период)	более 5, но менее или равно 10	III	III

Продолжение таблицы 4

№	Объект КИИ	Показатель	Значение показателя	Категория значи-мости	Итоговая категория значимости
2	Система бухгалтерского учета	Возникновение ущерба бюджетам РФ, оцениваемого: а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	III	III
		б) в снижении доходов бюджета субъекта РФ (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	III	
3	АСУ ТП основного производства	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	III	III
		Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые: а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	—	Без категории	
		б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	—	Без категории	

Продолжение таблицы 4

№	Объект КИИ	Показатель	Значение показателя	Категория значи-мости	Итоговая категория значимости
4	АСУ ТП вспомога-тельного производства	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	III	III
		Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые: а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	—	Без категории	

Полученные в ходе оценки данные, а также присвоенная категория значимости вносится в акт о результатах присвоения объекту КИИ категории значимости.

Сведения о результатах категорирования направляются в ФСТЭК в соответствии с Приказом ФСТЭК от 22 декабря 2017г. №236. [5]

Для дальнейшей работы был использован критический процесс — «Закупочная деятельность», и соответствующий ему объект КИИ — «Корпоративная сеть передачи данных» АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Акт о результатах присвоения объекту КИИ категории значимости должен содержать сведения об объекте КИИ, о программных и программно-аппаратных средствах, используемых на объекте КИИ, о взаимодействии объекта КИИ и сетей электросвязи, об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ, возможные последствия в случае

возникновения компьютерных инцидентов и реализованные организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры.

Сведения об объекте КИИ представлены в таблице 5.

Таблица 5 — Сведения об объекте КИИ

Наименование объекта	«Корпоративная сеть передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».
Адреса размещения объекта	442960, Пензенская область, г.Заречный, Проспект Мира, д.1
Сфера (область) деятельности, в которой функционирует объект	Оборонная промышленность
Назначение объекта	Обеспечение доступа удалённых пользователей к общим ресурсам сети.
Критические процессы, которые обеспечиваются объектом	Закупочная деятельность
Архитектура объекта	Сеть передачи данных

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ приведены в таблице 6.

Таблица 6 — Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ

Программно-аппаратные средства	Пользовательские компьютеры – 21 шт. Серверы – 4 шт. ПАК VipNet Coordinator HW – 10 шт.
Общесистемное программное обеспечение	Общесистемное программное обеспечение серверов: Windows Server 2008 R2 Standart. Общесистемное программное обеспечение клиентских ПЭВМ: Microsoft Windows 7 Professional.
Прикладное программное обеспечение	Пакет офисного ПО Libre Office; Архиватор 7-Zip; Файловый менеджер Double Commander; ПО для просмотра pdf-файлов Adobe Reader; ПО для просмотра изображений Picasa.
Программно-аппаратные средства	Пользовательские компьютеры – 21 шт. Серверы – 4 шт. ПАК VipNet Coordinator HW – 10 шт.

Продолжение таблицы 6

Средства защиты информации	СЗИ от НСД: «Secret Net 7 сервер безопасности», «Secret Net 7 клиент» Подсистема анализа защищённости: «MaxPatrol Scanner» СКЗИ: «ПАК VipNet Coordinator HW1000» Антивирусная защита: «Kaspersky Security Center 10»; «Kaspersky Endpoint Security 10»

Сведения о взаимодействии объекта КИИ и сетей электросвязи представлены в таблице 7.

Таблица 7 — Сведения о взаимодействии объекта КИИ и сетей электросвязи

Категория сети электросвязи	Выделенная сеть
Наименование оператора связи	Договор с АО «Гринатом» на оказание услуг: - Предоставление доступа к централизованным сервисам ЦОД и оказание телематических услуг через корпоративную сеть передачи данных; - Услуга по подключению узла корпоративной сети передачи данных к сети Оператора.
Цель взаимодействия с сетью электросвязи	Передача (прием) информации
Способ взаимодействия с сетью электросвязи	Проводной, TCP/IP

Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ представлены в таблице 8.

Таблица 8 — Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ

Категория нарушителя	Угрозы безопасности информации
Внутренний нарушитель, знающий все о системе и средствах её защиты.	Несанкционированное копирование защищаемой информации на неучтенные носители. Доступ к остаточной информации на жестком диске. Угрозы сканирования, направленные на выявление типа операционной системы АС, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др. Угрозы выявления паролей. Угрозы получения НСД путем подмены доверенного объекта. Угрозы внедрения ложного объекта как в АС, так и во внешних сетях. Угрозы типа «Отказ в обслуживании». Угрозы удаленного запуска приложений. Угрозы навязывание ложного маршрута сети.

Возможные последствия в случае возникновения компьютерных инцидентов представлены в таблице 9.

Таблица 9 — Возможные последствия в случае возникновения компьютерных инцидентов

Типы компьютерных инцидентов	Отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта.

Реализованные организационные и технические меры, применяемые для

обеспечения безопасности объекта критической информационной инфраструктуры представлены в таблице 10.

Таблица 10 — Реализованные организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ

Организационные меры	— установлена контролируемая зона, осуществляется контроль физического доступа к объекту; — разработаны документы (регламенты, инструкции, руководства) по обеспечению безопасности объекта; — определен порядок учета, выдачи, использования и хранения съемных магнитных носителей информации; — определен порядок проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ.
Технические меры	СЗИ от НСД: «Secret Net 7 сервер безопасности», «Secret Net 7 клиент». Подсистема анализа защищённости: «MaxPatrol Scanner». СКЗИ: «ПАК VipNet Coordinator HW1000». Антивирусная защита: «Kaspersky Security Center 10»; «Kaspersky Endpoint Security 10».

Акт о результатах присвоения критическим процессам объекта КИИ категории значимости представлен в приложении В.

Акт о результатах присвоения объекту КИИ категории значимости представлен в приложении Г.

4 Создание системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры

Цель системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры (СОИБ ЗОКИИ) — обеспечить ее устойчивое функционирование. Средства и методы должны соответствовать категории значимости, необходимо следить за их адекватностью для противодействия угрозам безопасности информации. Система обеспечения безопасности, функционирует до процесса вывода значимого объекта КИИ из эксплуатации. Всё время функционирования СОИБ развивается. В целом алгоритм создания и функционирования СОИБ ЗОКИИ представлен на рисунке 1.

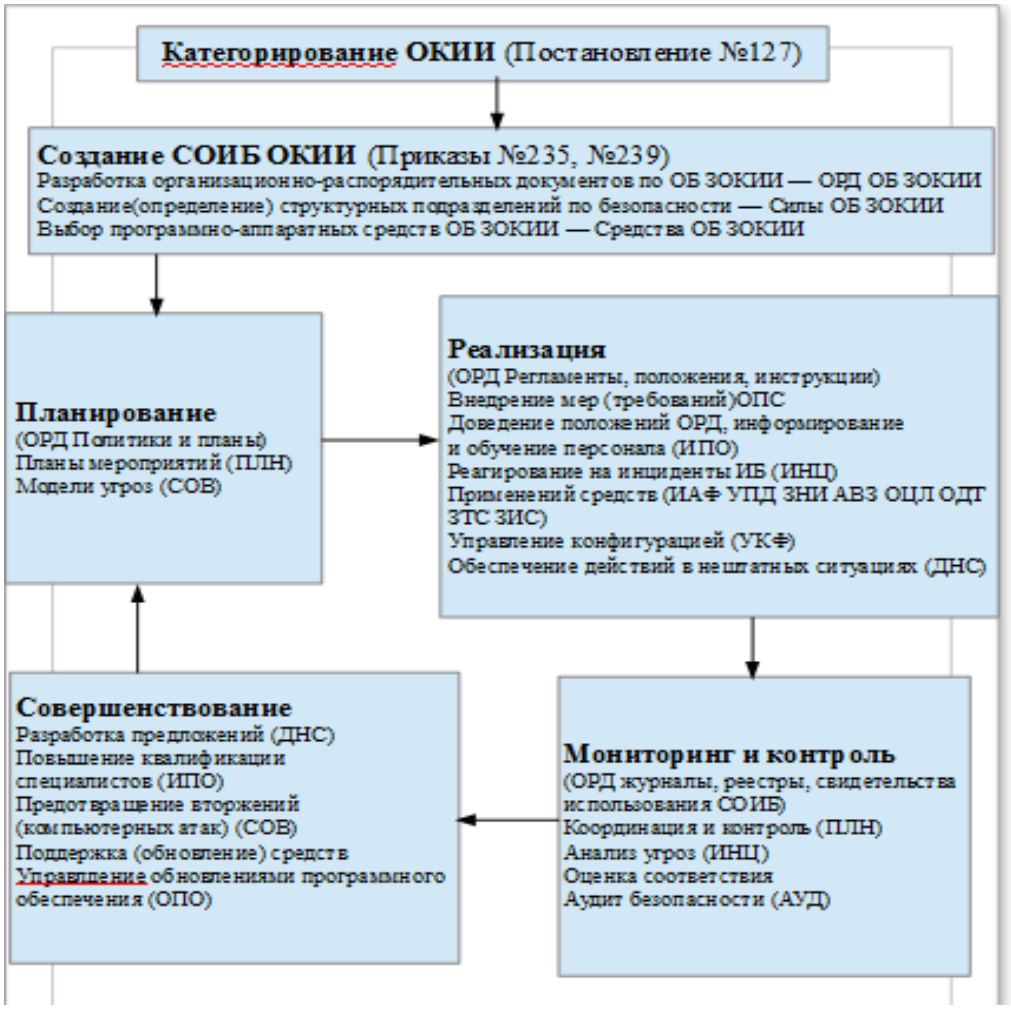

Рисунок 1 – Алгоритм создания и функционирования СОИБ ЗОКИИ

Этап 1. Планирование. На данном этапе устанавливаются требования, необходимые к выполнению для обеспечения безопасности каждого ЗОКИИ, а так же создается план мероприятий.

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. №187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1] ФСТЭК России устанавливает требования по обеспечению безопасности ЗОКИИ.

Требования к созданию СОИБ ЗОКИИ установлены приказом ФСТЭК России от 21 декабря 2017 г. № 235 [6], в котором определены состав сил обеспечения информационной безопасности их структура и функции, требования к ним. Необходимо проводить анализ угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры и выявлять уязвимости в них. Ошибки в результатах анализа приводят к неверной реализации СОИБ КИИ.

Организационно-распорядительные документы по безопасности ЗОКИИ, являются частью документов по вопросам обеспечения информационной безопасности субъекта КИИ. Положения, которые определяют порядок, а так же правила обеспечения безопасности ЗОКИИ, могут быть включены в общие документы по вопросам обеспечения информационной безопасности, и могут являться частью документов по вопросам функционирования ЗОКИИ.

Приказом ФСТЭК России от 25 декабря 2017 г. № 239 [7] утверждены требования по обеспечению безопасности ЗОКИИ.

Модель угроз безопасности информации может разрабатываться для нескольких ЗОКИИ, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

Этап 2. Реализация. На данном этапе осуществляется внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности ЗОКИИ (п. 34 приказа ФСТЭК России от 21 декабря 2017 г. № 235). [6]

Состав организационных и технических мер по обеспечению безопасности ЗОКИИ подробно приведен в приложении к приказу ФСТЭК России № 239 от 25 декабря 2017 г. [7]

Этап 3. Мониторинг и контроль. Основной целью проведения аудита информационной безопасности, является определение текущего состояния информационной безопасности и какие действия необходимо предпринять в дальнейшем для создания или улучшения системы защиты информации.

Этапы проведения аудита информационной безопасности (ИБ):

- инициирование аудита ИБ;
- заочное обследование;
- подготовка к очному обследованию;
- очное обследование;
- разработка отчета об аудите ИБ;
- завершение аудита ИБ.

Проведение аудита ИБ является базовой мерой обеспечения безопасности для ЗОКИИ, которая влияет на принятие решения о модернизации СОИБ. Результаты аудита, составляют основу для формирования технического задания и технического проектирование необходимых систем (подсистем) защиты или доработки существующих.

Этап 4. Совершенствование. Система защиты должна противостоять угрозам не только на данный момент, но и в дальнейшем. Не достаточно только факта внедрения процессов, обеспечивающих функционирование системы безопасности, процессы должны постоянно совершенствоваться.

В процессе совершенствования безопасности ЗОКИИ структурное подразделение по безопасности, а так же специалисты по безопасности должны проводить анализ функционирования системы безопасности и состояния безопасности ЗОКИИ, по результатам которого создавать предложения по

развитию системы безопасности и меры по модернизации безопасности ЗОКИИ.

Приказ о создании системы безопасности значимых объектов КИИ представлен в приложении Д.

Приказ о назначении ответственных за обеспечение безопасности значимых объектов КИИ представлен в приложении Е.

5 Установка требований, которые необходимо выполнить для обеспечения безопасности каждого значимого объекта критической информационной инфраструктуры и формирование плана мероприятий

Требования к созданию системы безопасности значимых объектов критической информационной инфраструктуры (СБ ЗОКИИ) установлены приказом ФСТЭК России от 21 декабря 2017 г. № 235 [6], в котором определены состав сил обеспечения информационной безопасности, их структура и функции, требования к ним.

Требования к созданию СБ ЗОКИИ.

Системы безопасности создаются субъектами КИИ и включают в себя правовые, организационные, технические и иные меры, направленные на обеспечение информационной безопасности (защиты информации) субъектов КИИ.

Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования значимых объектов КИИ при проведении в отношении них компьютерных атак.

Системы безопасности включают силы обеспечения безопасности значимых объектов критической информационной инфраструктуры и используемые ими средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Системы безопасности должны функционировать в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов КИИ, разрабатываемыми субъектами КИИ.

Системы безопасности должны обеспечивать:

– предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами КИИ, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

– недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов КИИ;

– восстановление функционирования значимых объектов КИИ, в том числе за счет создания и хранения резервных копий необходимой для этого информации;

– непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которое осуществляется в соответствии со статьей 5 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации". [1]

Создаваемые системы безопасности должны соответствовать требованиям, предъявляемым к:

– силам обеспечения безопасности ЗОКИИ;

– программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

– организационно-распорядительным документам по безопасности ЗОКИИ;

– функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ.

Состав сил обеспечения информационной безопасности:

– подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры;

– подразделения (работники), эксплуатирующие значимые объекты критической информационной инфраструктуры;

– подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) значимых объектов критической

информационной инфраструктуры;

– иные подразделения (работники), участвующие в обеспечении безопасности значимых объектов критической информационной инфраструктуры. [6]

План проведения мероприятий по обеспечению безопасности значимых объектов КИИ представлен в приложении Ж.

6 Моделирование угроз безопасности информации на значимых объектах критической информационной инфраструктуры

6.1 Моделирование угроз безопасности. Общие положения

Приказом ФСТЭК России от 25.12.2017 г. № 239 [7] утверждены требования по обеспечению безопасности значимых объектов КИИ. Ключевым требованием, установленным данным приказом, является моделирование угроз безопасности значимых объектов КИИ. В соответствии с данными требованиями модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта.

6.2 Модель нарушителя

Источниками угроз безопасности информации могут быть субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Источники угроз безопасности информации могут быть следующих типов:

— антропогенные источники (антропогенные угрозы);

— техногенные источники (техногенные угрозы);

— стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

— лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в корпоративной сети передачи данных, или нарушения функционирования корпоративной сети

передачи данных или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);

— лица, имеющие доступ к корпоративной сети передачи данных, непреднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации. Для «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» наиболее вероятны следующие виды нарушителей:

- спецслужбы иностранных государств (блоков государств);
- террористические, экстремистские группировки;
- разработчики, производители, поставщики программных, технических и программно-технических средств;
- лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;
- лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора;
- пользователи ИС;
- администраторы ИС и администраторы безопасности.

В качестве основных уровней знаний нарушителей об информационной системе можно выделить следующие:

- общая информация – информации о назначении и общих характеристиках ИС;

– эксплуатационная информация – информация, полученная из эксплуатационной документации;

– чувствительная информация – информация, дополняющая эксплуатационную информацию об ИС (например, сведения из проектной документации ИС).

В частности, нарушитель может иметь:

– данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИС;

– сведения об информационных ресурсах ИС — порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

– данные об уязвимостях, включая данные о недокументированных (не декларированных) возможностях технических, программных и программно-технических средств ИС;

– данные о реализованных в программных средствах защиты информации принципах и алгоритмах;

– исходные тексты программного обеспечения ИС;

– сведения о возможных каналах реализации угроз;

– информацию о способах реализации угроз.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

Предполагается, что нарушитель имеет:

– аппаратные компоненты системы защиты информации;

– доступные в свободной продаже технические средства и программное обеспечение;

– специально разработанные технические средства и программное

обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз информационной безопасности, а также возможности по их применению зависят от многих факторов, включая реализованные в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой системы защиты предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Оценка возможностей нарушителей отражена в модели нарушителя в таблице 11.

Таблица 11 — Модель нарушителя

№	Вид нарушителя	Тип наруши-теля	Возможные цели (мотивация) реализации угроз безопасности
1	спецслужбы иностранных государств (блоков государств)	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
4	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутрен-ний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
5	Лица, обеспечивающие функционирование ИС или обслуживающие инфраструктуру оператора;	Внутрен-ний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
6	Пользователи информационной системы;	Внутрен-ний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
7	Администраторы информационной системы и администраторы безопасности.	Внутрен-ний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, которые требуются для реализации угроз безопасности информации в ИС.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

– нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в ИС;

– нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в ИС;

– нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в ИС.

Потенциал нарушителей и их возможности представлены в таблице 12.

Таблица 12 — Потенциал и возможности нарушителей

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	лица, обеспечивающие функционирование ИС или обслуживающих инфраструктуру оператора, пользователи ИС, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент ИС, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на ИС
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы ИС и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах ЗИ, применяемых в ИС данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент ИС путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонент общесистемного ПО. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования ИС.

Продолжение таблицы 12

№	Потенциал наруши-телей	Виды нарушителей	Возможности по реализации угроз безопасности информации
3	Наруши-тели с высоким потен-циалом	спецслужбы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

Модель нарушителя безопасности информации «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» в

виде документа приведена в приложении И.

6.3 Определение актуальности угроз безопасности информации

Под угрозами безопасности информации при их обработке в ИС понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на неё.

Система защиты информации включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности информации и информационных технологий, используемых в ИС.

Под актуальными угрозами безопасности информации понимается совокупность условий и факторов, которые создают актуальную опасность несанкционированного, а так же случайного, доступа к информации при их обработке в ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также другие неправомерные действия.

Потенциальные угрозы безопасности информации:

- естественные угрозы (угрозы, вызванные воздействиями на ИС и её элементы объективных физических процессов или стихийных природных явлений, независящих от человека);
- искусственные угрозы (угрозы ИС, вызванные деятельностью человека). Среди них, исходя их мотивации действий, можно выделить:
  - непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и её элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
  - преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Актуальной считается угроза, которая может быть реализована в ИС и

представляет опасность для защищаемой информации.

Для оценки возможности реализации угрозы применяются два показателя:

- уровень исходной защищенности информационной системы;
- частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности информационной системы понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС, представленных в таблице 13.

Таблица 13 — Показатель исходной защищенности ИС

Технические и эксплуатационные характеристики	Уровень защищенности		
	Высокий	Средний	Низкий
1 По территориальному размещению			
Локальная ИС, развернутая в пределах нескольких близко расположенных зданий		+	
2 По наличию соединения с сетями общего пользования:			
ИС имеющая одноточечный выход в сеть общего пользования;		+	
3 По встроенным (легальным) операциям с записями баз персональных данных:			
запись, удаление, сортировка;		+	
4 По разграничению доступа к защищаемой информации:			
ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС.		+	
5 По наличию соединений с другими базами данных иных систем:			
интегрированная ИСПДн (организация использует несколько баз данных ИС, при этом организация не является владельцем всех используемых баз данных);			+
6 По уровню обобщения (обезличивания) информации:			
Информационная система, в которой предоставленные данные пользователю не являются обезличенными;			+
7 По объему информации. Которая предоставляется сторонним пользователям без предварительной обработки:			
ИС, предоставляющая часть информации.		+	

Исходная степень защищенности определяется следующим образом:

– ИС имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИС соответствует уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – по среднему уровню защищенности (положительные решения по второму столбцу);

– ИС имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИС соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – к низкому уровню защищенности;

– ИС имеет низкую степень защищенности, если не выполняются условия по пунктам 1 и 2.

Исходя из данных представленных в таблице 13, пять характеристик ИС (71,4%) соответствуют среднему уровню защищенности, две (28,56%) – низкому. Из этого следует, что ИС имеет средний уровень исходной защищенности.

При составлении перечня актуальных угроз безопасности, каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y1, а именно:

– 0 для высокой степени исходной защищенности;

– 5 для средней степени исходной защищенности;

– 10 для низкой степени исходной защищенности.

Числовой коэффициент уровня исходной защищенности ИС Y1 равно 5.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для данной ИС в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;

– низкая вероятность – объективные предпосылки для осуществления угрозы существуют, но принятые меры существенно затрудняют ее реализацию;

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны;

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности информации не приняты.

При составлении перечня актуальных угроз безопасности информации каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

– 0 для маловероятной угрозы;

– 2 для низкой вероятности угрозы;

– 5 для средней вероятности угрозы;

– 10 для высокой вероятности угрозы.

Информация о вероятности реализации угроз безопасности информации, обрабатываемой в информационной системе, приведены в таблице 12.

Возможность реализации угрозы определяется коэффициентом реализуемости угрозы Y, значение которого определяется соотношением:

$$Y = (Y1 + Y2)/20 \qquad (1)$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если Y больше 0, но меньше 0,3, то возможность реализации угрозы признается низкой;

– если Y больше 0,3, но меньше 0,6, то возможность реализации угрозы признается средней;

– если Y больше 0,6, но меньше 0,8, то возможность реализации

угрозы признается высокой;

– если Y больше 0,8, то возможность реализации угрозы признается очень высокой.

Данные о возможности реализации угроз безопасности информации, обрабатываемой в ИС, представлены в таблице 15.

При оценке опасности угрозы определяется вербальный показатель опасности для ИС. Этот показатель имеет три значения:

– низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям;

– средняя опасность – если реализация угрозы может привести к негативным последствиям;

– высокая опасность – если реализация угрозы может привести к значительным негативным последствиям.

Данные по оценке опасности угроз безопасности информации, обрабатываемой в ИС, представлены в таблице 15.

Определение актуальности угроз безопасности информации, проводится в соответствии с правилами, приведенными в таблице 14.

Таблица 14 – Правила отнесения угроз безопасности информации к актуальным

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

Данные по оценке актуальности угроз безопасности информации, обрабатываемой в ИС, представлены в таблице 15.

Таблица 15 — Данные по оценке актуальности угроз безопасности информации

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
			Вероятность (частота) реализации угрозы	Обоснование	Вероятность возникновения угрозы (Y2)				
1	Угроза автоматического распространения вредоносного кода в грид-системе УБИ.001								Технология не применяется в данной ИС
2	Угроза агрегирования данных, передаваемых в грид-системе УБИ.002								Технология не применяется в данной ИС
3	Угроза анализа криптографических алгоритмов и их реализации УБИ. 003	5	маловероятно	На создаваемом АП отсутствует криптографическое ПО. Отсутствие у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	0	0,25	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
4	Угроза аппаратного сброса пароля BIOS УБИ. 004	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
5	Угроза внедрения вредоносного кода в BIOS УБИ. 005	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	2	0,35	Низкая	Низкая	Неактуальная
6	Угроза внедрения кода или данных УБИ.006	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	2	0,35	Низкая	Низкая	Неактуальная
7	Угроза воздействия на программы с высокими привилегиями УБИ. 007	5	низкая	Отсутствие административных привилегий у пользователя Наличие доверенного канала связи посредством СКЗИ. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
8	Угроза восстановления аутентификационной информации УБИ. 008	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
9	Угроза восстановления предыдущей уязвимой версии BIOS УБИ. 009	5	низкая	На АП установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
10	Угроза выхода процесса за пределы виртуальной машины УБИ.010								Данная угроза не применяется к рассматриваемой ИС
11	Угроза деавторизации санкционированного клиента беспроводной сети УБИ.011								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
12	Угроза деструктивного изменения конфигурации/среды окружения программ УБИ.012	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
13	Угроза деструктивного использования декларированного функционала BIOS УБИ.013	5	низкая	На АП установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
14	Угроза длительного удержания вычислительных ресурсов пользователями УБИ.014	5	низкая	Использование на АП базового проверенного набора ПО. Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
15	Угроза доступа к защищаемым файлам с использованием обходного пути УБИ.015	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
16	Угроза доступа к локальным файлам сервера при помощи URL УБИ.016	5	низкая	Отсутствие у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	2	0,35	Низкая	Низкая	Неактуальная
17	Угроза доступа/перехвата/изменения HTTP cookies УБИ.017	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к защищаемой информации	5	0,5	Средняя	Средняя	Актуальная
18	Угроза загрузки нештатной операционной системы УБИ.018	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	Низкая	Низкая	Неактуальная
19	Угроза заражения DNS-кеша УБИ.019	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
20	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг УБИ.20								Технология не применяется в данной ИС
21	Угроза злоупотребления доверием потребителей облачных услуг УБИ.21								Технология не применяется в данной ИС
22	Угроза избыточного выделения оперативной памяти УБИ.022	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО. Возможность выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
23	Угроза изменения компонентов информационной (автоматизированной) системы УБИ.023	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
24	Угроза изменения режимов работы аппаратных элементов компьютера УБИ.024	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
25	Угроза изменения системных и глобальных переменных УБИ.025	5	низкая	Отсутствие возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
26	Угроза искажения XML-схемы УБИ.026	5	средняя	Наличие доверенного канала связи посредством СКЗИ Возможность изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером.	5	0,5	Средняя	Средняя	Актуальная
27	Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027	5	средняя	Возможность дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
28	Угроза использования альтернативных путей доступа к ресурсам УБИ.028	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).	5	0,5	Средняя	Средняя	Актуальная
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами УБИ.029								Технология не применяется в данной ИС
30	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию УБИ.030	5	средняя	Наличие у нарушителя сведений о производителе/модели объекта защиты (ОЗ) и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для ОЗ;	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
31	Угроза использования механизмов авторизации для повышения привилегий УБИ.031	5	средняя	Возможность получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа	5	0,5	Средняя	Средняя	Актуальная
32	Угроза использования поддельных цифровых подписей BIOS УБИ.032	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
33	Угроза использования слабостей кодирования входных данных УБИ.033	5	низкая	Возможность осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.).	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
34	Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Наличие доверенного канала связи посредством СКЗИ	5	0,5	Средняя	Средняя	Актуальная
35	Угроза использования слабых криптографических алгоритмов BIOS УБИ.035	5	низкая	Сложность использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI.	2	0,35	Низкая	Низкая	Неактуальная
36	Угроза исследования механизмов работы программы УБИ.036	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
37	Угроза исследования приложения через отчёты об ошибках УБИ.037	5	низкая	Отсутствие у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	2	0,35	Низкая	Низкая	Неактуальная
38	Угроза исчерпания вычислительных ресурсов хранилища больших данных УБИ.038								Технология не применяется в данной ИС
39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS УБИ.039	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя	2	0,35	Низкая	Низкая	Неактуальная
40	Угроза конфликта юрисдикций различных стран УБИ.40								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
41	Угроза межсайтового скриптинга УБИ.041								Технология не применяется в данной ИС
42	Угроза межсайтовой подделки запроса УБИ.042								Данная угроза не применяется к рассматриваемой ИС
43	Угроза нарушения доступности облачного сервера УБИ.043								Технология не применяется в данной ИС
44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины УБИ.044								Данная угроза не применяется к рассматриваемой ИС
45	Угроза нарушения изоляции среды исполнения BIOS УБИ.045	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия УБИ.046								Данная угроза не применяется к рассматриваемой ИС
47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке УБИ.047								Технология не применяется в данной ИС
48	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин УБИ.048								Данная угроза не применяется к рассматриваемой ИС
49	Угроза нарушения целостности данных кеша УБИ.049	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных УБИ.050								Технология не применяется в данной ИС
51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания УБИ.051	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения УБИ.052								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
53	Угроза невозможности управления правами пользователей BIOS УБИ.053	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
54	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг УБИ.054								Технология не применяется в данной ИС
55	Угроза незащищённого администрирования облачных услуг УБИ.055								Технология не применяется в данной ИС
56	Угроза некачественного переноса инфраструктуры в облако УБИ.056								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
57	Угроза неконтролируемого копирования данных внутри хранилища больших данных УБИ.057								Технология не применяется в данной ИС
58	Угроза неконтролируемого роста числа виртуальных машин УБИ.058								Технология не применяется в данной ИС
59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.059								Технология не применяется в данной ИС
60	Угроза неконтролируемого уничтожения информации хранилищем больших данных УБИ.060								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
61	Угроза некорректного задания структуры данных транзакции УБИ.061	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера УБИ.062								Данная угроза не применяется к рассматриваемой ИС
63	Угроза некорректного использования функционала программного и аппаратного обеспечения УБИ.063	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя	2	0,35	Низкая	Низкая	Неактуальная
64	Угроза некорректной реализации политики лицензирования в облаке УБИ.064								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
65	Угроза неопределённости в распределении ответственности между ролями в облаке УБИ.065								Технология не применяется в данной ИС
66	Угроза неопределённости ответственности за обеспечение безопасности облака УБИ.066								Технология не применяется в данной ИС
67	Угроза неправомерного ознакомления с защищаемой информацией УБИ.067	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
68	Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением УБИ.068	5	средняя	Отсутствие возможность осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
69	Угроза неправомерных действий в каналах связи УБИ.069	5	средняя	Возможность несанкционированного доступа к сетевому трафику у нарушителя	5	0,5	Средняя	Средняя	Актуальная
70	Угроза непрерывной модернизации облачной инфраструктуры УБИ.070								Технология не применяется в данной ИС
71	Угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071	5	средняя	Удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных; Технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; Информация не хранится в криптографически преобразованном виде	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS УБИ.072	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети УБИ.073								Технология не применяется в данной ИС
74	Угроза несанкционированного доступа к аутентификационной информации УБИ.074	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	низкая	низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
75	Угроза несанкционированного доступа к виртуальным каналам передачи УБИ.075								Технология не применяется в данной ИС
76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети УБИ.076								Технология не применяется в данной ИС
77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение УБИ.077								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети УБИ.078								Технология не применяется в данной ИС
79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин УБИ.079								Технология не применяется в данной ИС
80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети УБИ.080								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
81	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы УБИ.081								Технология не применяется в данной ИС
82	Угроза несанкционированного доступа к сегментам вычислительного поля УБИ.082								Данная угроза не применяется к рассматриваемой ИС
83	Угроза несанкционированного доступа к системе по беспроводным каналам УБИ.083								Данная угроза не применяется к рассматриваемой ИС
84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети УБИ.084								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации УБИ.085								Технология не применяется в данной ИС
86	Угроза несанкционированного изменения аутентификационной информации УБИ.086	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
87	Угроза несанкционированного использования привилегированных функций BIOS УБИ.087	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
88	Угроза несанкционированного копирования защищаемой информации УБИ.088	5	средняя	Контроль со стороны ответственных за эксплуатацию ТС ИС. Возможность неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).	5	0,5	Средняя	Средняя	Актуальная
89	Угроза несанкционированного редактирования реестра УБИ.089	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
90	Угроза несанкционированного создания учётной записи пользователя УБИ.090	5	низкая	Отсутствие прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	2	0,35	Низкая	Низкая	Неактуальная
91	Угроза несанкционированного удаления защищаемой информации УБИ.091	5	низкая	Использование на АП базового проверенного набора ПО. Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам УБИ.092								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
93	Угроза несанкционированного управления буфером УБИ.093	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
94	Угроза несанкционированного управления синхронизацией и состоянием УБИ.094	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации. Возможность изменения нарушителем последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния ИС, или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.).	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
95	Угроза несанкционированного управления указателями УБИ.095	5	низкая	Предоставление прав доступа к информационным ресурсам информационной системы по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
96	Угроза несогласованности политик безопасности элементов облачной инфраструктуры УБИ.096								Технология не применяется в данной ИС
97	Угроза несогласованности правил доступа к большим данным УБИ.097	5	низкая	Использования политик безопасности, согласованных между собой.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098	5	средняя	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика. Возможность определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
99	Угроза обнаружения хостов УБИ.099	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика. Сканирование нарушителем вычислительной сети для выявления работающих сетевых узлов.	2	0,35	Низкая	Низкая	Неактуальная
100	Угроза обхода некорректно настроенных механизмов аутентификации УБИ.100	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации.	2	0,35	Низкая	Низкая	Неактуальная
101	Угроза общедоступности облачной инфраструктуры УБИ.101								Технология не применяется в данной ИС
102	Угроза опосредованного управления группой программ через совместно используемые данные УБИ.102	5	низкая	Возможность опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные и др.)	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
103	Угроза определения типов объектов защиты УБИ.103	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика.	2	0,35	Низкая	Низкая	Неактуальная
104	Угроза определения топологии вычислительной сети УБИ.104	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Возможность определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.	2	0,35	Низкая	Низкая	Неактуальная
105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных УБИ.105								Технология не применяется в данной ИС
106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера УБИ.106								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
107	Угроза отключения контрольных датчиков УБИ.107								Данная угроза не применяется к рассматриваемой ИС
108	Угроза ошибки обновления гипервизора УБИ.108								Технология не применяется в данной ИС
109	Угроза перебора всех настроек и параметров приложения УБИ.109	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность получения нарушителем доступа к дополнительному скрытому функционалу или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
110	Угроза перегрузки грид-системы вычислительными заданиями УБИ.110								Технология не применяется в данной ИС
111	Угроза передачи данных по скрытым каналам УБИ.111								Данная угроза не применяется к рассматриваемой ИС
112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением УБИ.112								Данная угроза не применяется к рассматриваемой ИС
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники УБИ.113	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
114	Угроза переполнения целочисленных переменных УБИ.114	5	низкая	Отсутствие у внешнего нарушителя сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных. Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации УБИ.115	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Отсутствие у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	2	0,35	Низкая	Низкая	Неактуальная
116	Угроза перехвата данных, передаваемых по вычислительной сети УБИ.116	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
117	Угроза перехвата привилегированного потока УБИ.117	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
118	Угроза перехвата привилегированного процесса УБИ.118	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
119	Угроза перехвата управления гипервизором УБИ.119								Технология не применяется в данной ИС
120	Угроза перехвата управления средой виртуализации УБИ.120								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
121	Угроза повреждения системного реестра УБИ.121	5	низкая	Возникновение ошибок в работе отдельных процессов или всей операционной системы. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
122	Угроза повышения привилегий УБИ.122	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
123	Угроза подбора пароля BIOS УБИ.123	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
124	Угроза подделки записей журнала регистрации событий УБИ.124	5	низкая	Технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
125	Угроза подключения к беспроводной сети в обход процедуры аутентификации УБИ.125								Данная угроза не применяется к рассматриваемой ИС
126	Угроза подмены беспроводного клиента или точки доступа УБИ.126								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
127	Угроза подмены действия пользователя путём обмана УБИ.127	5	низкая	Применение методов борьбы с социальной инженерией. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
128	Угроза подмены доверенного пользователя УБИ.128	5	низкая	Возможность нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
129	Угроза подмены резервной копии программного обеспечения BIOS УБИ.129	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Отсутствие возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии ПО BIOS/UEFI, предварительно подменённой нарушителем.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
130	Угроза подмены содержимого сетевых ресурсов УБИ.130								Данная угроза не применяется к рассматриваемой ИС
131	Угроза подмены субъекта сетевого доступа УБИ.131								Данная угроза не применяется к рассматриваемой ИС
132	Угроза получения предварительной информации об объекте защиты УБИ.132								Данная угроза не применяется к рассматриваемой ИС
133	Угроза получения сведений о владельце беспроводного устройства УБИ.133								Технология не применяется в данной ИС
134	Угроза потери доверия к поставщику облачных услуг УБИ.134								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
135	Угроза потери и утечки данных, обрабатываемых в облаке УБИ.135								Технология не применяется в данной ИС
136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных УБИ.136								Технология не применяется в данной ИС
137	Угроза потери управления облачными ресурсами УБИ.137								Технология не применяется в данной ИС
138	Угроза потери управления собственной инфраструктурой при переносе её в облако УБИ.138								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
139	Угроза преодоления физической защиты УБИ.139	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Контроль физического доступа (наличие замков в помещении, обученный проинструктированный персонал и т.п.). Отсутствие возможности любого из методов проникновения на объект	2	0,35	Низкая	Низкая	Неактуальная
140	Угроза приведения системы в состояние «отказ в обслуживании» УБИ.140	5	низкая	Возможность отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов.	2	0,35	Низкая	Низкая	Неактуальная
141	Угроза привязки к поставщику облачных услуг УБИ.141								Технология не применяется в данной ИС
142	Угроза приостановки оказания облачных услуг вследствие технических сбоев УБИ.142								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.143	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
144	Угроза программного сброса пароля BIOS УБИ.144	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Отсутствие в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля	2	0,35	Низкая	Низкая	Неактуальная
145	Угроза пропуска проверки целостности программного обеспечения УБИ.145	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера УБИ.146								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
147	Угроза распространения несанкционированно повышенных прав на всю грид-систему УБИ.147								Технология не применяется в данной ИС
148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных УБИ.148								Технология не применяется в данной ИС
149	Угроза сбоя обработки специальным образом изменённых файлов УБИ.149	5	низкая	Отсутствие у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке;	2	0,35	Низкая	Низкая	Неактуальная
150	Угроза сбоя процесса обновления BIOS УБИ.150	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL УБИ.151	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Возможность получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера.	2	0,35	Низкая	Низкая	Неактуальная
152	Угроза удаления аутентификационной информации УБИ.152	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов УБИ.153	5	низкая	Отсутствие у нарушителя сведений о сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов. Отсутствие у нарушителя сведений о сетевом адресе дискредитируемой системы.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS УБИ.154	5	низкая	Установка и использование проверенного ПО. Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
155	Угроза утраты вычислительных ресурсов УБИ.155	5	низкая	Отсутствие у нарушителя сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы	2	0,35	Низкая	Низкая	Неактуальная
156	Угроза утраты носителей информации УБИ.156	5	низкая	Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.157	5	низкая	Отсутствие возможности получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.) Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
158	Угроза форматирования носителей информации УБИ.158	5	низкая	Создание резервных копий информации, хранящейся на носителях.	2	0,35	Низкая	Низкая	Неактуальная
159	Угроза «форсированного веб-браузинга» УБИ.159								

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.160	5	низкая	Отсутствие у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации. Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями УБИ.161								Технология не применяется в данной ИС
162	Угроза эксплуатации цифровой подписи программного кода УБИ.162	5	низкая	В системах не используются цифровые подписи кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма прописывания программного кода	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
163	Угроза перехвата исключения/сигнала из привилегированного блока функций УБИ.163	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре УБИ.164								Технология не применяется в данной ИС
165	Угроза включения в проект не достоверно испытанных компонентов УБИ.165	5	низкая	Для применения в системе выбираются компоненты в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Использование сертифицированного ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
166	Угроза внедрения системной избыточности УБИ.166	5	низкая	Отсутствие избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект) программного обеспечения (или системы в целом).	2	0,35	Низкая	Низкая	Неактуальная
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов УБИ.167								Данная угроза не применяется к рассматриваемой ИС
168	Угроза «кражи» учётной записи доступа к сетевым сервисам УБИ.168								Данная угроза не применяется к рассматриваемой ИС
169	Угроза наличия механизмов разработчика УБИ.169	5	низкая	Использование проверенного ПО, не подразумевающего использования отладочных механизмов	2	0,35	Низкая	Низкая	Неактуальная
170	Угроза неправомерного шифрования информации УБИ.170	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
171	Угроза скрытного включения вычислительного устройства в состав бот-сети УБИ.171								Технология не применяется в данной ИС
172	Угроза распространения «почтовых червей» УБИ.172								Данная угроза не применяется к рассматриваемой ИС
173	Угроза «спама» веб-сервера УБИ.173								Данная угроза не применяется к рассматриваемой ИС
174	Угроза «фарминга» УБИ.174								Данная угроза не применяется к рассматриваемой ИС
175	Угроза «фишинга» УБИ.175								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты УБИ.176	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью УБИ.177	5	низкая	Отсутствие (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора» Предоставление прав пользователю в минимально достаточном объем.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
178	Угроза несанкционированного использования системных и сетевых утилит УБИ.178	5	низкая	Предоставление прав пользователю в минимально достаточном объем. Отсутствие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему, предназначенных для использования администратором для диагностики и обслуживания системы	2	0,35	Низкая	Низкая	Неактуальная
179	Угроза несанкционированной модификации защищаемой информации УБИ.179	5	низкая	Предоставление прав пользователю в минимально достаточном объеме. Контроль со стороны ответственных за эксплуатацию ТС ИС. Использование доверенно-го канала связи СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
180	Угроза отказа подсистемы обеспечения температурного режима УБИ.180	5	низкая	Реализация угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
181	Угроза перехвата одноразовых паролей в режиме реального времени УБИ.181	5	низкая	Отсутствие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия. Невозможность осуществления нарушителем перехвата трафика между системой и пользователем, ввиду использования доверенного канала связи СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
182	Угроза физического устаревания аппаратных компонентов УБИ.182	5	низкая	Возможность нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций).	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
183	Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.183								Данная угроза не применяется к рассматриваемой ИС
184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства УБИ.184								Технология не применяется в данной ИС
185	Угроза несанкционированного изменения параметров настройки средств защиты информации УБИ.185	5	низкая	Отсутствие СЗИ, вследствие этого отсутствие у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	2	0,35	Низкая	Низкая	Неактуальная
186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент УБИ.186								Данная угроза не применяется к рассматриваемой ИС
187	Угроза несанкционированного воздействия на средство защиты информации УБИ.187	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
188	Угроза подмены программного обеспечения УБИ.188								Данная угроза не применяется к рассматриваемой ИС
189	Угроза маскирования действий вредоносного кода УБИ.189	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная
190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет УБИ.190								Данная угроза не применяется к рассматриваемой ИС
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения УБИ.191	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объем	2	0,35	Низкая	Низкая	Неактуальная
192	Угроза использования уязвимых версий программного обеспечения УБИ.192	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объем	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика УБИ.193	5	низкая	Использование на АП базового проверенного набора ПО. Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
194	Угроза несанкционированного использования привилегированных функций мобильного устройства УБИ.194								Технология не применяется в данной ИС
195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.195								Данная угроза не применяется к рассматриваемой ИС
196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве УБИ.196								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
197	Угроза хищения аутентификационной информации из временных файлов cookie УБИ.197	5	низкая	Использование на АП базового проверенного набора ПО. На АП закрыт RDP-порт.	2	0,35	Низкая	Низкая	Неактуальная
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов УБИ.198	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объем На АП закрыт RDP-порт.	2	0,35	Низкая	Низкая	Неактуальная
199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.199								Технология не применяется в данной ИС
200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.200								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере УБИ.201	5	низкая	Использование защищенного канала связи СКЗИ Настройка браузера в режиме, в котором не активирована функция автоматического заполнения форм авторизации	2	0,35	Низкая	Низкая	Неактуальная
202	Угроза несанкционированной установки приложений на мобильные устройства УБИ.202								Технология не применяется в данной ИС
203	Угроза утечки информации с неподключенных к сети Интернет компьютеров УБИ.203								Данная угроза не применяется к рассматриваемой ИС
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров УБИ.204								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты УБИ.205	5	низкая	Возможность нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов.	2	0,35	Низкая	Низкая	Неактуальная
206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем УБИ.206								Данная угроза не применяется к рассматриваемой ИС
207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) УБИ.207								Данная угроза не применяется к рассматриваемой ИС
208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники УБИ.208								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора УБИ.209								Данная угроза не применяется к рассматриваемой ИС
210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения УБИ.210								Данная угроза не применяется к рассматриваемой ИС
211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем УБИ.211								Данная угроза не применяется к рассматриваемой ИС
212	Угроза перехвата управления информационной системой УБИ.212								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
213	Угроза обхода многофакторной аутентификации УБИ.213								Данная угроза не применяется к рассматриваемой ИС
214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации УБИ.214								Данная угроза не применяется к рассматриваемой ИС
215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов УБИ.215								Данная угроза не применяется к рассматриваемой ИС
216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах УБИ.216								Технология не применяется в данной ИС

Продолжение таблицы 15

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения УБИ.217								Данная угроза не применяется к рассматриваемой ИС

Исходя из результатов определения актуальности угроз, содержащихся в таблице 15, для ИС актуальными являются следующие угрозы:

– угроза доступа/перехвата/изменения HTTP cookies УБИ.017;

– угроза искажения XML-схемы УБИ.026;

– угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027;

– угроза использования альтернативных путей доступа к ресурсам УБИ.028;

– угроза использования информации идентификации/аутентификации, заданной по умолчанию УБИ.030;

– угроза использования механизмов авторизации для повышения привилегий УБИ.031;

– угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034;

– угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.068;

– угроза неправомерных действий в каналах связи УБИ.069;

– угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071;

– угроза несанкционированного копирования защищаемой информации УБИ.088;

– угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098;

– угроза физического устаревания аппаратных компонентов УБИ.182.

6.4 Описание актуальных угроз безопасности информации

Затем было выполнено описание актуальных угроз безопасности информации.

Описание каждой угрозы безопасности информации должно включать:

– источник угрозы безопасности информации;

– уязвимости, которые могут быть использованы для реализации угрозы безопасности информации;

– возможные сценарии реализации угрозы безопасности информации;

– возможные последствия от реализации (возникновения) угрозы безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации должен использоваться банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России. [8]

Описание актуальных угроз безопасности приведено в таблице 16.

Модель угроз безопасности информации «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» представлена в приложении К.

Таблица 16 — Описание актуальных угроз безопасности информации

№	Угрозы безопасности	Источник угроз	Уязвимости	Сценарии	Последствия
1	Угроза доступа/перехвата/ изменения HTTP cookies УБИ.017	Внешний нарушитель с низким потенциалом	BDU:2018-00868: Уязвимость браузера Firefox, связанная с ошибками реализации хранилища файлов cookies, позволяющая нарушителю получить доступ к файлам cookies httpOnly	Несанкционированный доступ к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя)	Нарушение конфиден-циальности и доступности
2	Угроза искажения XML-схемы УБИ.026	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	BDU:2020-00402: Уязвимость компонента XML Parsing XML-редактора Easy XML Editor, позволяющая нарушителю вызвать отказ в обслуживании приложения или осуществить чтение произвольных файлов в системе	Изменение нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером.	Нарушение целостности и доступности
3	Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027	Внутренний нарушитель с низким потенциалом Внешний нарушитель с высоким потенциалом	BDU:2020-02177: Уязвимость компонента Microsoft Windows Graphics операционных систем Windows, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации	Дезинформирование пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации; подмена или искажение информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства	Нарушение целостности

Продолжение таблицы 16

№	Угрозы безопасности	Источник угроз	Уязвимости	Сценарии	Последствия
4	Угроза использования альтернативных путей доступа к ресурсам УБИ.028	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2020-02199: Уязвимость службы Work Folder Service операционных систем Windows, позволяющая нарушителю повысить свои привилегии	Несанкционированный доступ к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса)	Нарушение конфиден-циальности
5	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию УБИ.030	Внутренний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	BDU:2017-02221: Уязвимость микропрограммного обеспечения маршрутизатора Axesstel MU553S, связанная с использованием по умолчанию стандартного пароля для учётной записи администратора, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность данных	Прохождение нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты	Нарушение конфиден-циальности, целостности и доступности
6	Угроза использования механизмов авторизации для повышения привилегий УБИ.031	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2019-01295: Уязвимость системы управления базами данных PostgreSQL, связанная с ошибками авторизации, позволяющая нарушителю повысить свои привилегии	Получение доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа	Нарушение конфиден-циальности

Продолжение таблицы 16

№	Угрозы безопасности	Источник у	Уязвимости	Сценарии	Последствия
7	Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034	Внешний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2019-03486: Уязвимость реализации сетевого протокола Microsoft Server Message Block (SMB) операционных систем Windows, позволяющая нарушителю раскрыть защищаемую информацию	Несанкционированный доступ к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов	Нарушение конфиден-циальности,целостности и доступности
8	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.068	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	BDU:2019-04302: Уязвимость компонента API браузера Firefox, позволяющая нарушителю подменить пользовательский интерфейс	Осуществление нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API).	Нарушение конфиден-циальности, целостности и доступности
9	Угроза неправомерных действий в каналах связи УБИ.069	Внешний нарушитель с низким потенциалом	BDU:2017-01098: Уязвимость протокола SMBv1 операционной системы Microsoft Windows, позволяющая нарушителю выполнить произвольный код	Внесение нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи	Нарушение конфиден-циальности и целостности
10	Угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2020-02196: Уязвимость драйвера базы данных Microsoft JET Database Engine операционных систем Windows, позволяющая нарушителю выполнить произвольный код	Осуществление прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации	Нарушение конфиден-циальности

Продолжение таблицы 16

№	Угрозы безопасности	Источник угроз	Уязвимости	Сценарии	Последствия
11	Угроза несанкционированного копирования защищаемой информации УБИ.088	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2020-01826: Уязвимость браузера Firefox, связанная с неправильным назначением прав доступа для критического ресурса, позволяющая нарушителю получить несанкционированный доступ к информации	Неправомерное получение нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы	Нарушение конфиденциальности
12	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098	Внешний нарушитель с низким потенциалом	BDU:2017-01328: Уязвимость операционной системы Windows, позволяющая нарушителю выполнить произвольный код	Определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов	Нарушение конфиденциальности
13	Угроза физического устаревания аппаратных компонентов УБИ.182	Внутренний нарушитель с низким потенциалом	Чувствительность к влажности, пыли, загрязнению	Нарушение функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания, обусловленного влиянием физической окружаю-щей среды (влажности, пыли, коррозийных субстанций).	Нарушение доступности

7 Внедрение организационных и технических мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры

7.1 Базовый набор мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры

В соответствии с требованиями Постановления Правительства Российской Федерации от 8 февраля 2018 г. N 127 [3], комиссия по категорированию, назначенная в Приказе «О создании комиссии по категорированию», установила III категорию значимости для объекта критической информационной инфраструктуры «Корпоративная сеть передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

При определении базового набора мер по обеспечению безопасности значимого объекта КИИ для III категории значимости использовался Приказ ФСТЭК России от 25 декабря 2017 г. N 239. [7] Базовый набор мер представлен в приложении Л.

7.2 Техническое задание на создание системы безопасности значимого объекта

Для выполнения требований к обеспечению информационной безопасности объекта критической информационной инфраструктуры, необходимо выполнить адаптацию базового набора мер с угрозами безопасности информации, и определить меры, которые обеспечивают нейтрализацию угроз безопасности информации с соответствующей категорией значимости объекта критической информационной инфраструктуры. Требования к обеспечению информационной безопасности включаются в техническое задание (ТЗ) на создание системы безопасности значимого объекта критической информационной инфраструктуры.

В процессе разработки технического задания на разработку системы безопасности значимого объекта критической информационной инфраструктуры должны быть определены цели, задачи защиты значимого объекта, категория значимости данного объекта, выполнены организационные и технические меры, стадии и этапы работ, требования к системе защиты и перечень нормативных документов по защите объектов критической информационной инфраструктуры.

В ходе адаптации базового набора мер по обеспечению безопасности значимого объекта КИИ были исключены следующие меры защиты:

– ИАФ.5 Идентификация и аутентификация внешних пользователей, так как внешние пользователи не имеют доступ к системе;

– УПД.13 Реализация защищенного удаленного доступа, так как к системе не применяется удаленный доступ;

– УПД.14 Контроль доступа из внешних информационных (автоматизированных) систем, так как к системе нет доступа из внешних информационных (автоматизированных) систем;

– ЗИС.038 Защита информации при использовании мобильных устройств, так как в системе не используются мобильные устройства;

– ЗИС.39 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных, так как в системе нет виртуальных машин.

Адаптированный базовый набор мер защиты информации по обеспечению безопасности значимого объекта КИИ «Корпоративной сети передачи данных» АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» приведен в таблице 17.

Таблица 17— Адаптированный базовый набор мер защиты информации

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
		3
I. Идентификация и аутентификация (ИАФ)		
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+
ИАФ.2	Идентификация и аутентификация устройств	+
ИАФ.3	Управление идентификаторами	+
ИАФ.4	Управление средствами аутентификации	+
ИАФ.7	Защита аутентификационной информации при передаче	+
II. Управление доступом (УПД)		
УПД.0	Регламентация правил и процедур управления доступом	+
УПД.1	Управление учетными записями пользователей	+
УПД.2	Реализация модели управления доступом	+
УПД.4	Разделение полномочий (ролей) пользователей	+
УПД.5	Назначение минимально необходимых прав и привилегий	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+
ЗНИ.1	Учет машинных носителей информации	+
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+

Продолжение таблицы 17

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+
V. Аудит безопасности (АУД)		
АУД.0	Регламентация правил и процедур аудита безопасности	+
АУД.1	Инвентаризация информационных ресурсов	+
АУД.2	Анализ уязвимостей и их устранение	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+
АУД.4	Регистрация событий безопасности	+
АУД.6	Защита информации о событиях безопасности	+
АУД.7	Мониторинг безопасности	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+
АУД.10	Проведение внутренних аудитов	+
VI. Антивирусная защита (АВЗ)		
АВЗ.0	Регламентация правил и процедур антивирусной защиты	+
АВЗ.1	Реализация антивирусной защиты	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+
VIII. Обеспечение целостности (ОЦЛ)		
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+

Продолжение таблицы 17

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ОЦЛ.1	Контроль целостности программного обеспечения	+
IX. Обеспечение доступности (ОДТ)		
ОДТ.0	Регламентация правил и процедур обеспечения доступности	+
ОДТ.4	Резервное копирование информации	+
ОДТ.5	Обеспечение возможности восстановления информации	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+
X. Защита технических средств (ЗТС)		
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+
ЗТС.2	Организация контролируемой зоны	+
ЗТС.3	Управление физическим доступом	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+
ЗТС.5	Защита от внешних воздействий	+
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)		
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+

Продолжение таблицы 17

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+
ЗИС.5	Организация демилитаризованной зоны	+
ЗИС.6	Управление сетевыми потоками	+
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+
ЗИС.19	Защита информации при ее передаче по каналам связи	+
ЗИС.20	Обеспечение доверенных канала, маршрута	+
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+
ЗИС.32	Защита беспроводных соединений	+
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+
ЗИС.35	Управление сетевыми соединениями	+
XII. Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+
ИНЦ.1	Выявление компьютерных инцидентов	+
ИНЦ.2	Информирование о компьютерных инцидентах	+
ИНЦ.3	Анализ компьютерных инцидентов	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+
XIII. Управление конфигурацией (УКФ)		
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+

Продолжение таблицы 17

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
УКФ.2	Управление изменениями	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+
XIV. Управление обновлениями программного обеспечения (ОПО)		
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+
ОПО.3	Тестирование обновлений программного обеспечения	+
ОПО.4	Установка обновлений программного обеспечения	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)		
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+
ДНС.1	Разработка плана действий в нештатных ситуациях	+
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+
XVII. Информирование и обучение персонала (ИПО)		
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+

Продолжение таблицы 17

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+
ИПО.2	Обучение персонала правилам безопасной работы	+
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+

Техническое задание на создание системы безопасности значимого объекта представлено в приложении М.

8 Описание взаимодействия субъекта критической информационной инфраструктуры с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) — это единый централизованный, территориально-распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак. [10]

ГосСОПКА необходимо создавать для обмена информацией о компьютерных атаках на информационные системы, нарушение или прекращение работы которых может негативно отразиться на экономике или безопасности страны.

Согласно Указу Президента Российской Федерации от 15.01.2013 г. № 31с [9] основными задачами ГосСОПКА являются:

– прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

– обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

– реализация контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

– выявление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Центры ГосСОПКА являются ведомственными или корпоративными.

Ведомственные центры ГосСОПКА создаются органами государственной

власти (ОГВ), и организациями, которые осуществляют лицензируемую деятельность в области защиты информации в интересах ОГВ для защиты их информационных ресурсов.

Корпоративные центры ГосСОПКА (КЦ ГосСОПКА) создаются государственными корпорациями, операторами связи либо иными организациями, которые осуществляют лицензируемую деятельность в области защиты информации, в собственных интересах, и для оказания услуг по предупреждению, обнаружению и ликвидации последствий компьютерных атак.

В составе центров ГосСОПКА могут присутствовать структурные элементы — центры мониторинга, которые организованы по территориальному принципу, такие центры могут образовывать иерархическую структуру, которая отражает, например, территориальную или организационную структуру субъекта ГосСОПКА.

Главный центр — наивысшая структура в иерархии, которая разрабатывает нормативные документы и методики. За работу центра отвечает ФСБ России.

Головной центр — наивысшая структура в иерархии центров, которые объединяются по ведомственному или организационному признакам.

Подчинённый центр — центр, который структурно подчиняется головному центру.

Сегмент ГосСОПКА образуют центр ГосСОПКА и иерархически подчиненные ему центры мониторинга.

При взаимодействии сегментов ГосСОПКА с Национальным координационным центром по компьютерным инцидентам происходит обмен сведениями о компьютерных инцидентах, индикаторами компрометации и методическими рекомендациями по обнаружению, предупреждению и ликвидации последствий типовых компьютерных атак.

К ГосСОПКА должны подключаться владельцы объектов КИИ. [10]

Зона ответственности КЦ ГосСОПКА:

– силы, средства, а так же объекты критической информационной инфраструктуры АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», КЦ ГосСОПКА, по отношению к которым КЦ ГосСОПКА обеспечивает обнаружение, реагирование, предупреждение и ликвидацию последствий компьютерных атак;

– информационный обмен между КЦ ГосСОПКА и национальным координационным центром по компьютерным инцидентам (НКЦКИ).

Корпоративные центры ГосСОПКА должны осуществлять следующие функции:

– реализация мероприятий по обнаружению, реагированию, предупреждению и ликвидации компьютерных атак в Корпоративном сегменте ГосСОПКА;

– мониторинг и регистрация событий информационной безопасности;

– регистрация, а так же сбор и анализ сведений об инцидентах информационной безопасности на объектах критической информационной инфраструктуры;

– выполнение мероприятий по предупреждению, реагированию и ликвидации последствий инцидентов информационной безопасности и компьютерных атак на объектах критической информационной инфраструктуры;

– обнаружение, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;

– своевременное обновление средств, предназначенных для функционирования КЦ ГосСОПКА, выявление ошибок в их работе;

– поддержание в актуальном состоянии информации об объектах критической информационной инфраструктуры, включая оборудование и программное обеспечение;

– предоставление в НКЦКИ сведений об инцидентах информационной безопасности на объектах критической информационной инфраструктуры и о предпринятых мерах;

– передача в НКЦКИ сведений о степени защищенности объектов критической информационной инфраструктуры;

– оказание содействия Субъекту по реагированию и ликвидации последствий компьютерных инцидентов и атак;

– уведомление Субъекта об инцидентах информационной безопасности и компьютерных атаках, и оказание содействия по устранению причин их возникновения;

– предоставление Субъекту информации об актуальных уязвимостях, полученных от НКЦКИ.

КЦ ГосСОПКА имеет право:

– направлять уведомления и запросы Субъекту по вопросам, связанным с обнаружением, реагированием, предупреждением и ликвидацией последствий компьютерных атак;

– проводить проверку материалов, которые предоставляет Субъект;

– формировать предложения по совершенствованию нормативной правовой базы по защите информации.

Зона ответственности Субъекта:

– силы и средства, а так же объекты критической информационной инфраструктуры, в отношении которых Субъект обеспечивает обнаружение, реагирование, предупреждение и ликвидацию последствий компьютерных атак;

– информационный обмен между КЦ ГосСОПКА, Субъектом и НКЦКИ.

Субъект КИИ при взаимодействии с центрами ГосСОПКА должен осуществлять следующие функции:

– определение перечня объектов критической информационной инфраструктуры, необходимого для подключения к технической инфраструктуре КЦ ГосСОПКА;

– мониторинг событий информационной безопасности на объектах критической информационной инфраструктуры;

– регистрация инцидентов информационной безопасности;

– реализация сбора и анализа сведений об уязвимостях программного обеспечения и оборудования;

– проведение мероприятий по предупреждению, реагированию и ликвидации последствий компьютерных инцидентов и компьютерных атак;

– формирование информации об объектах критической информационной инфраструктуры, а так же оборудование и программное обеспечение;

– реализация полученных от КЦ ГосСОПКА рекомендаций по противодействию компьютерным атакам и устранению уязвимостей;

– осуществление информационного взаимодействия с региональными центрами НКЦКИ по вопросам предупреждения, реагирования, и ликвидации последствий инцидентов и компьютерных атак.

Субъект должен направить в КЦ ГосСОПКА:

– заявку на подключение к КЦ ГосСОПКА;

– перечень объектов критической информационной инфраструктуры, с указанием категории значимости;

– перечень используемого оборудования и программного обеспечения;

– перечень используемых средств защиты информации;

– список лиц ответственных за обнаружение, реагирование, предупреждение, и ликвидации последствий компьютерных атак.

Субъект должен предоставлять в КЦ ГосСОПКА:

– сведения об инцидентах информационной безопасности и компьютерных атаках, а так же информации о предпринятых мерах;

– сведения об актуальных уязвимостях;

– информацию о составе объектов критической информационной инфраструктуры.

Субъект имеет право:

– направлять запрос в КЦ ГосСОПКА по рекомендациям о ликвидации последствий компьютерных атак;

– формировать предложения по совершенствованию нормативной правовой базы по защите информации.

Способы информирования КЦ ГосСОПКА:

– по телекоммуникационным каналам связи;

– по электронной почте;

– посредством телефонной связи.

Сроки информирования.

Информация, связанная с функционированием объектов критической информационной инфраструктуры, направляется Субъектом в КЦ ГосСОПКА, не позднее 3-х часов с момента обнаружения компьютерного инцидента.

Приказ об организации взаимодействия с ГосСОПКА представлен в приложении Н.

9 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Значительную часть времени, специалист по защите информации проводит за компьютером. Во время работы за компьютером специалист перерабатывает большой объем информации и постоянно концентрирует внимание, исходя из этого при долговременной работе за компьютером часто развивается психологическая усталость и эмоциональные нарушения. Так же к вредным психофизиологическим факторам, влияющим на нервную систему специалиста, относятся интеллектуальные нагрузки, однообразие труда, высокий уровень электромагнитных излучений.

Так как работа за компьютером, является чисто интеллектуальным трудом, то нервная система принимает основную часть нагрузки. Из за долгой работы за компьютером может возникать хроническое переутомление, следствием чего являются расстройство внимания и невозможность концентрироваться.

Высокий уровень электромагнитных излучений часто приводит к повышенной активности нервной системы, которая проявляется, как нарушение сна, и может привести к эмоциональной нестабильности. В следствии чего возможно развитие упадка сил. Поэтому при длительном воздействии таких излучений на специалиста характерны следующие симптомы: головные были, слабость, быстрая утомляемость и ухудшение самочувствия в целом. Данные симптомы выражаются в разной степени.

Для снижения воздействия вредных психофизиологических факторов, которые влияют на нервную систему специалиста по защите информации, необходимы регулярные перерывы в работе. Через 40 минут работы за компьютером необходим перерыв на 10 минут.

Рекомендуется во время перерывов выполнять упражнения для расслабления. Так, при ощущении сонливости или утомляемости, необходимо выполнять такие упражнения как: круговые вращения головой, повороты головы в стороны и перевод взгляда с ближних объектов на дальние.

При головных болях необходимо выполнять такие упражнения как: круговые вращения головой, концентрирование взгляда на разных углах помещения, перевод взгляда с ближних объектов на дальние, потягивания всем телом и круговые вращения плечами.

При повышенной раздражительности необходимо выполнять такие упражнения как: перевод взгляда с ближних объектов на дальние, концентрирование взгляда на разных углах помещения. [11]

Заключение

В ходе выполнения выпускной квалификационной работы были определены процессы субъекта КИИ и выявлены среди них критические, так же определены объекты КИИ, необходимые для данных критических процессов. Проведено категорирование значимого объекта КИИ.

Создана система обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры. Установлены требования, которые необходимо выполнить для обеспечения безопасности каждого значимого объекта критической информационной инфраструктуры и сформирован план мероприятий. Выполнено моделирование угроз безопасности информации на значимом объекте критической информационной инфраструктуры, внедрение организационных и технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Был описан процесс взаимодействия субъекта КИИ с центрами ГосСОПКА.

Были изучены вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации, так же методы и средства физической культуры, которые снижают их воздействие.

Таким образом, задание на выпускную квалификационную работу были выполнены в полном объеме.

Протокол проверки на оригинальность представлен в приложении П.

Список использованных источников

1 Федеральный закон от 26 июля 2017 г. N 187-ФЗ [Электронный ресурс]. — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения 12.04.2020)

2 Категорирование объектов КИИ [Электронный ресурс]. — Режим доступа: https://infosecuritydays.ru (дата обращения 14.04.2020)

3 Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127 [Электронный ресурс]. — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/287-postanovleniya/1614-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127 (дата обращения 18.04.2020)

4 Информационное сообщение ФСТЭК от 24 августа 2018 года N 240/25/3752 [Электронный ресурс]. — Режим доступа: http://docs.cntd.ru/document/560324037 (дата обращения 18.04.2020)

5 Приказ ФСТЭК России от 22 декабря 2017 г. N 236 [Электронный ресурс]. — Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236 (дата обращения 18.04.2020)

6 Приказ ФСТЭК России от 21 декабря 2017 г. N 235 [Электронный ресурс]. — Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236 (дата обращения 18.04.2020)

7 Приказ ФСТЭК России от 25 декабря 2017 г. N 239 [Электронный ресурс] — Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения

18.04.2020)

8 Банк данных угроз безопасности информации [Электронный ресурс] — Режим доступа: http://bdu.fstec.ru/ubi/vul (дата обращения 20.04.2020)

9 Указ Президента Российской Федерации от 15.01.2013 г. № 31с [Электронный ресурс]. — Режим доступа: http://www.kremlin.ru/acts/bank/36691 (дата обращения 05.05.2020)

10 Подключение к ГосСОПКА [Электронный ресурс]. — Режим доступа: https://amonitoring.ru/service/gossopka/ (дата обращения 05.05.2020)

11 Основные вредные факторы, влияющие на состояние здоровья людей, работающих за компьютером [Электронный ресурс]. — Режим доступа: https://xn--80ahc0abogjs.com/valeologiya_739/osnovnyie-vrednyie-faktoryi-vliyayuschie.html (дата обращения 15.05.2020)

Приложение А

(обязательное)

Приказ о создании комиссии по категорированию

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

г. Заречный

« __ » _____ 20__г. № ____

ПРИКАЗ

о создании комиссии по категорированию

В целях исполнения требований Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановления Правительства РФ от 8 февраля 2018г. №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а так же перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»,

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию по категорированию объектов критической информационной инфраструктуры, принадлежащих АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на праве собственности, аренды или ином законном основании.
2. Председателем комиссии назначить Фамилия И.О. – должность.
3. В состав комиссии включить:

– Фамилия И.О. – должность;

– Фамилия И.О. – должность;

– Фамилия И.О. – должность.

4. Комиссии в срок до 28.05.2020г.:

– определить процессы в рамках осуществления видов деятельности АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»;

– выявить критические процессы у АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»;

– выявить объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

– подготовить предложения для включения объектов критической информационной инфраструктуры в перечень объектов критической информационной инфраструктуры, подлежащих категорированию;

– представить на утверждение перечень объектов критической информационной инфраструктуры, подлежащих категорированию, в срок до 20.05.2020г.;

– рассмотреть возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

– проанализировать угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

– установить каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принять решение об отсутствии необходимости присвоения им категорий значимости;

– представить на утверждение акты по результатам категорирования;

– представить на утверждение сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

5. Ознакомить с настоящим приказом председателя и членов создаваемой комиссии.

6. Контроль за исполнением настоящего приказа оставляю за собой.

7. Приказ вступает в силу со дня его регистрации.

Генеральный директор АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» Фамилия И.О.

Приложение Б

(обязательное)

Перечень объектов критической информационной инфраструктуры

УТВЕРЖДАЮ

_____ _____

Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____

Подпись руководителя субъекта или уполномоченного им лица | Фамилия, имя, отчество руководителя субъекта или уполномоченного им лица

«__» _____ 20__г.

Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)
1	Корпоративная сеть	ИС	Экономическая сфера	01.06.20г.	Фамилия И.О. т.00-00-00
2	Система бухгалтерского учета	ИС	Экономическая сфера	01.06.20г.	Фамилия И.О. т.00-00-00
3	АСУ ТП основного производства	АСУ ТП	оборонная промышленность	01.06.20г.	Фамилия И.О. т.00-00-00
4	АСУ ТП вспомогательного производства	АСУ ТП	оборонная промышленность	01.06.20г.	Фамилия И.О. т.00-00-00

Приложение В

(обязательное)

«Акт о результатах присвоения критическим процессам объекта критической информационной инфраструктуры категории значимости»

АО «ФНПЦ «ПО «СТАРТ» ИМ. М.В. ПРОЦЕНКО»

№_____

СОГЛАСОВАНО	УТВЕРЖДАЮ
Должность	Должность
_____Фамилия И.О.	_____Фамилия И.О.
«___» _____ 20__ г.	«___» _____ 20__ г.

АКТ

о результатах присвоения критическим процессам объекта критической информационной инфраструктуры категории значимости

Заречный 2020

Комиссия по категорированию, созданная приказом по предприятию, в целях реализации требований Федерального закона от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановления Правительства РФ от 08.02.2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», провела оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов на объекте КИИ — «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» по установленным критическим процессам субъекта КИИ, определила значения показателей значимости критических процессов субъекта КИИ и присвоила критическим процессам субъекта КИИ одну из категорий значимости, что представлено в таблице В.1.

Таблица В.1 — Критический процесс: «Закупочная деятельность»

Показатель		**Значение показателя**			
		III категория	II категория	I категория	Без категории
	I. Социальная значимость				
1	Причинение ущерба жизни и здоровью людей (человек)	— (более или равно 1, но менее или равно 50)	— (более 50, но менее или равно 500)	— (более 500)	—
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:	—	—	—	—

Продолжение таблицы В.1

Показатель		Значение показателя			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	— (вся территория одного муниципального образования или одной внутригородской территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутриго-родской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта РФ или территории города федерального значения)	—
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:	—	—	—	—
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	— (вся территория одного муниципального образования или одной внутригородской территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения)	—
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
4.	Прекращение или нарушение функционирования сети связи, оцениваемые:	—	—	—	—

Продолжение таблицы В.1

Показатель	Значение показателя			
а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;	— (вся территория одного муниципального образования или одной внутригородской территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения)	— (выход за пределы территории одного субъекта РФ или территории города федерального значения)	—
б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
5. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	— (менее или равно 24, но более 12)	— (менее или равно 12, но более 6)	— (менее 6)	—
II. Политическая значимость				
6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	— (прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения)	— (прекращение или нарушение функционирования федерального органа государственной власти)	— (прекращение или нарушение функционирования Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ)	—

Продолжение таблицы В.1

Показатель		Значение показателя			
7	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора РФ	— (нарушение условий договора межведомственного характера (срыв переговоров или подписания))	— (нарушение условий межправительственного договора (срыв переговоров или подписания))	— (нарушение условий межгосударственного договора (срыв переговоров или подписания))	—
	III. Экономическая значимость				
8.	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	+ (более 5, но менее или равно 10)	— (более 10, но менее или равно 15)	— (более 15)	III категория
9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого:	—	—	—	—
	а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	— (более 0,001, но менее или равно 0,05)	— (более 0,05, но менее или равно 0,1)	— (более 0,1)	—
	б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);	— (более 0,001, но менее или равно 0,05)	— (более 0,05, но менее или равно 0,1)	— (более 0,1)	—

Продолжение таблицы В.1

Показатель	Значение показателя			
в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	—	(более 0,01, но менее или равно 0,5)	(более 0,5, но менее или равно 1)	(более 1)
10 Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)	—	(более 3, но менее или равно 70)	(более 70, но менее или равно 120)	(более 120)
IV. Экологическая значимость				
11. Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:	—	—	—	—

Продолжение таблицы В.1

Показатель	Значение показателя			
а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	— (вся территория одного муниципального образования или одной внутригородской территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта РФ или территории города федерального значения)	—
б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12. Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	— (прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта РФ или города федерального значения)	— (прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации)	— (прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ)	—
13. Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:				

Продолжение таблицы В.1

Показатель	**Значение показателя**			
а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	+ (более 5, но менее или равно 10)	— (более 10, но менее или равно 15)	— (более 15)	III категория
б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	+ (более 3, но менее или равно 10)	— (более 10, но менее или равно 40)	— (более 40)	III категория
14. Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	— (менее или равно 4, но более 2)	— (менее или равно 2, но более 1)	— (более 1)	—

Председатель комиссии: _____
(ФИО, подпись)

Члены комиссии: _____
(ФИО, подпись)

_____
(ФИО, подпись)

_____
(ФИО, подпись)

Приложение Г

(обязательное)

«Акт о результатах присвоения объекту критической информационной инфраструктуры категории значимости»

УТВЕРЖДАЮ

_____

руководитель организации

_____

подпись, инициалы, фамилия

«___» _____ 20__ г.

АКТ

о результатах присвоения объекту критической информационной инфраструктуры категории значимости

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

(наименование объекта)

На основании приказа от «___» _____20__г. № __ комиссия в составе:

председатель комиссии: _____

(роль, должность, фамилия, инициалы)

члены комиссии: _____

(роль, должность, фамилия, инициалы)

_____

(роль, должность, фамилия, инициалы)

_____

(роль, должность, фамилия, инициалы)

в соответствии с требованиями Федерального закона от 26.07.2017 №187, Постановления Правительства РФ от 08.02.2018г. №127, провела категорирование объекта критической информационной инфраструктуры «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

В ходе работы комиссия по категорированию определила:

1. Сведения об объекте критической информационной инфраструктуры (далее – КИИ), представленные в Приложении 1;

2. Сведения об угрозах безопасности информации объекта КИИ, представленные в Приложении 2;

3. Реализованные на объекте КИИ меры по обеспечению безопасности, представленные в Приложении 3;

4. Масштаб возможных последствий в случае возникновения компьютерных инцидентов в соответствии с перечнем показателей критериев значимости, представленный в Приложении 4.

На основании результата анализа значений показателей критериев значимости объекта КИИ в соответствии с постановлением Правительства РФ от 08.02.2018 №127 объекту «Корпоративная сеть передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» присвоена III категория.

Председатель комиссии: _____
(ФИО, подпись)

Члены комиссии: _____
(ФИО, подпись)

_____
(ФИО, подпись)

_____
(ФИО, подпись)

Приложение 1

Сведения об объекте КИИ представлены в таблице Г.1.

Таблица Г.1 — Сведения об объекте КИИ

Наименование объекта	«Корпоративная сеть передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».
Адреса размещения объекта	442960, Пензенская область, г. Заречный, Проспект Мира, д.1
Сфера (область) деятельности, в которой функционирует объект	Оборонная промышленность
Назначение объекта	Обеспечение доступа удалённых пользователей к общим ресурсам сети.
Критические процессы, которые обеспечиваются объектом	Закупочная деятельность
Архитектура объекта	Сеть передачи данных

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ представлены в таблице Г.2.

Таблица Г.2 — Сведения о программных и программно-аппаратных средствах

Программно-аппаратные средства	Пользовательские компьютеры – 21 шт. Серверы – 4 шт. ПАК VipNet Coordinator HW – 10 шт.
Общесистемное программное обеспечение	Общесистемное программное обеспечение серверов: Windows Server 2008 R2 Standart. Общесистемное программное обеспечение клиентских ПЭВМ: Microsoft Windows 7 Professional.
Прикладное программное обеспечение	Пакет офисного ПО Libre Office; Архиватор 7-Zip; Файловый менеджер Double Commander; ПО для просмотра pdf-файлов Adobe Reader; ПО для просмотра изображений Picasa.
Средства защиты информации	СЗИ от НСД: «Secret Net 7 сервер безопасности», «Secret Net 7 клиент» Подсистема анализа защищённости: «MaxPatrol Scanner» СКЗИ: «ПАК VipNet Coordinator HW1000» Антивирусная защита: «Kaspersky Security Center 10»; «Kaspersky Endpoint Security 10»

Сведения о взаимодействии объекта КИИ и сетей электросвязи представлены в таблице Г.3.

Таблица Г.3 — Сведения о взаимодействии объекта КИИ и сетей электросвязи

Категория сети электросвязи	Выделенная сеть
Наименование оператора связи	Договор с АО «Гринатом» № 24/8977-Д от 07.05.2017 года на оказание услуг: - COM.18 Предоставление доступа к централизованным сервисам ЦОД и оказание телематических услуг через КСПД; - Услуга по подключению узла КСПД к сети Оператора.
Цель взаимодействия с сетью электросвязи	Передача (прием) информации
Способ взаимодействия с сетью электросвязи	Проводной, TCP/IP

Приложение 2

Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ представлены в таблице Г.4.

Таблица Г.4 — Сведения об угрозах безопасности информации и категориях нарушителей

Категория нарушителя	Угрозы безопасности информации
Внутренний нарушитель, знающий все о системе и средствах её защиты.	– несанкционированное копирование защищаемой информации на неучтенные носители; – доступ к остаточной информации на жестком диске; – угрозы сканирования, направленные на выявление типа операционной системы АС, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.; – угрозы выявления паролей; – угрозы получения НСД путем подмены доверенного объекта; – угрозы внедрения ложного объекта как в АС, так и во внешних сетях; – угрозы типа «Отказ в обслуживании»; – угрозы удаленного запуска приложений; – угрозы навязывание ложного маршрута сети.

Возможные последствия в случае возникновения компьютерных инцидентов представлены в таблице Г.5.

Таблица Г.5 — Возможные последствия в случае возникновения компьютерных инцидентов

Типы компьютерных инцидентов	Отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта.

Приложение 3

Реализованные организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ представлены в таблице Г.6.

Таблица Г.6 — Реализованные организационные и технические меры

Организационные меры	— установлена контролируемая зона, осуществляется контроль физического доступа к объекту; — разработаны документы (регламенты, инструкции, руководства) по обеспечению безопасности объекта; — определен порядок учета, выдачи, использования и хранения съемных магнитных носителей информации; — определен порядок проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ.
Технические меры	СЗИ от НСД: «Secret Net 7 сервер безопасности», «Secret Net 7 клиент». Подсистема анализа защищённости: «MaxPatrol Scanner». СКЗИ: «ПАК VipNet Coordinator HW1000». Антивирусная защита: «Kaspersky Security Center 10»; «Kaspersky Endpoint Security 10».

Приложение 4

Перечень показателей критериев значимости и их значения представлены в таблице Г.7.

Таблица Г.7 — Перечень показателей критериев значимости и их значения

	Показатель	**Значение показателя**			
		III категория	II категория	I категория	Без категории
	I. Социальная значимость				
1	Причинение ущерба жизни и здоровью людей (человек)	— (более или равно 1, но менее или равно 50)	— (более 50, но менее или равно 500)	— (более 500)	—
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:	—	—	—	—
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	— (вся территория одного муниципального образования или одной внутригородской территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта РФ или территории города федерального значения)	—
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:	—	—	—	—

Продолжение таблицы Г.7

Показатель	Значение показателя			
а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	— (вся территория одного муниципального образования или одной внутригородс-кой территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта РФ или территории города федерального значения)	—
б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
4. Прекращение или нарушение функционирования сети связи, оцениваемые:	—	—	—	—
а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;	— (вся территория одного муниципального образования или одной внутригородс-кой территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородс-кой территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения)	—
б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
5. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	— (менее или равно 24, но более 12)	— (менее или равно 12, но более 6)	— (менее 6)	—

Продолжение таблицы Г.7

Показатель	Значение показателя			
II. Политическая значимость				
6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	— (прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения)	— (прекращение или нарушение функционирования федерального органа государственной власти)	— (прекращение или нарушение функционирования Администрации Президента РФ, Правительства Российской Федерации, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ)	—
7. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	— (нарушение условий договора межведомственного характера (срыв переговоров или подписания))	— (нарушение условий межправительственного договора (срыв переговоров или подписания))	— (нарушение условий межгосударственного договора (срыв переговоров или подписания))	—
8. Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	+ (более 5, но менее или равно 10)	— (более 10, но менее или равно 15)	— (более 15)	III категория

Продолжение таблицы Г.7

Показатель				Значение показателя
III. Экономическая значимость				
9. Возникновение ущерба бюджетам Российской Федерации, оцениваемого:	—	—	—	—
а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	— (более 0,001, но менее или равно 0,05)	— (более 0,05, но менее или равно 0,1)	— (более 0,1)	—
б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);	— (более 0,001, но менее или равно 0,05)	— (более 0,05, но менее или равно 0,1)	— (более 0,1)	—
в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	— (более 0,01, но менее или равно 0,5)	— (более 0,5, но менее или равно 1)	— (более 1)	—
10 Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ, являющимся в соответствии с законодательством РФ системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений	— (более 3, но менее или равно 70)	— (более 70, но менее или равно 120)	— (более 120)	—
IV. Экологическая значимость				
11. Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:	—	—	—	—

Продолжение таблицы Г.7

Показатель	Значение показателя			
а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	— (вся территория одного муниципального образования или одной внутригородской территории города федерального значения)	— (выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта РФ или территории города федерального значения)	— (выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения)	—
б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	— (более или равно 50, но менее 1000)	— (более или равно 1000, но менее 5000)	— (более или равно 5000)	—
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12 Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	— (прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального значения)	— (прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации)	— (прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ)	—
13. Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:				
а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	+ (более 5, но менее или равно 10)	— (более 10, но менее или равно 15)	— (более 15)	III категория

Продолжение таблицы Г.7

Показатель	Значение показателя			
б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	+ (более 3, но менее или равно 10)	— (более 10, но менее или равно 40)	— (более 40)	III категория
14. Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	— (менее или равно 4, но более 2)	— (менее или равно 2, но более 1)	— (более 1)	—

Приложение Д

(обязательное)

«Приказ о создании системы безопасности значимых объектов критической информационной инфраструктуры»

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

г. Заречный

« __ » _____ 20__г. № ____

ПРИКАЗ

о создании системы безопасности значимых объектов критической информационной инфраструктуры

В целях исполнения требований Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Приказа ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»,

ПРИКАЗЫВАЮ:

1. Утвердить цели создания системы безопасности значимых объектов критической информационной инфраструктуры, основные этапы создания системы безопасности значимых объектов критической информационной инфраструктуры, принадлежащих АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» на праве собственности, аренды или ином законном основании.
2. Назначить ответственным лицом за создание системы безопасности значимых объектов КИИ Фамилия И.О.
3. Контроль за исполнением настоящего приказа оставляю за собой.
4. Приказ вступает в силу со дня его подписания.

Генеральный директор АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» _____ Фамилия И.О.

Приложение Е

(обязательное)

«Приказ о назначении ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры»

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

г. Заречный

« __ » _____ 20__г. № ____

ПРИКАЗ

о назначении ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры

С целью организации работ по обеспечению безопасности «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», в целях исполнения требований Федерального закона от 26.07.2017 №187-ФЗ, Приказа ФСТЭК России от 21 декабря 2017 г. № 235,

ПРИКАЗЫВАЮ:

1 Утвердить список лиц, ответственных за организацию работ и обеспечение безопасности «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» согласно приложению 1.

2 Контроль за исполнением настоящего приказа оставляю за собой.

3 Приказ вступает в силу со дня его подписания.

Генеральный директор АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» _____ Фамилия И.О.

Приложение 1

к приказу №____

«__» _____ 20__ г.

Список лиц, ответственных за организацию работ и обеспечение безопасности «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

ИС	ФИО	Должность
Корпоративная сеть передачи данных	Фамилия И.О.	Специалист по информационной безопасности
	Фамилия И.О.	Администратор ИБ

Приложение Ж

(обязательное)

План проведения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры

Утверждаю

_____

руководитель субъекта КИИ

«___» _____ 20___ г.

План проведения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры

№	Мероприятие	Ответственный	Срок
1	Назначение ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры	Фамилия И.О	25.04.20
2	Установление требований к обеспечению безопасности значимого объекта	Фамилия И.О	30.04.20
3	Моделирование угроз безопасности информации на значимых объектах критической информационной инфраструктуры	Фамилия И.О	15.05.20
4	Разработка организационных и технических мер по обеспечению безопасности значимого объекта	Фамилия И.О	25.05.20
5	Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие	Фамилия И.О	10.06.20
6	Разработка организационно-распорядительных документов по вопросам обеспечения безопасности критической информационной инфраструктуры	Фамилия И.О	20.06.20
7	Обеспечение безопасности значимого объекта в ходе его эксплуатации	Фамилия И.О	До вывода значимого объекта из эксплуатации

Приложение И

(обязательное)

Модель нарушителя

УТВЕРЖДЕНА

_____

(руководитель предприятия)

«___» _____ 20___ г..

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Корпоративной сети передачи данных»

ПРИНАДЛЕЖАЩЕЙ

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

Заречный 2020

1 Общие положения

В настоящей модели нарушителя описывается потенциальный нарушитель информационной безопасности «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко». Данная Модель разработана в соответствии с требованиями Федерального законодательства.

2 Назначение ИС

Корпоративная сеть передачи данных представляет собой сеть, которая взаимодействует с распределенной сетью Госкорпорации «Росатома», объединяющая в единое информационное пространство локальные сети предприятия.

3 Исходные данные об ИС

Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена: система, имеющая подключения к сетям общего пользования.

Режим обработки персональных данных: многопользовательский.

Режим разграничения прав доступа пользователей системы: система с разграничением прав доступа.

Объекты защиты:

1 Защищаемая информация.

2 Технологическая информация:

- управляющая информация;
- технологическая информация средств доступа к системам управления;
- информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;

– информационные ресурсы;

– служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации.

3 Программно-технические средства обработки:

– общесистемное и специальное программное обеспечение (операционные системы и другие);

– резервные копии общесистемного программного обеспечения;

– инструментальные средства и утилиты систем управления ресурсами ИС;

– аппаратные средства обработки информации.

4 Средства защиты информации:

– средства управления и разграничения доступа пользователей;

– средства обеспечения регистрации и учета действий с информацией;

– средства, обеспечивающие целостность данных;

– средства антивирусной защиты.

5 Объекты и помещения, в которых размещены компоненты ИС:

Местонахождение технических средств автоматизированной системы: в пределах РФ (город Заречный, Пензенская область, пр. Мира 1).

4 Модель нарушителя

По признаку принадлежности к корпоративной сети передачи данных все нарушители делятся на две группы:

– внешние нарушители;

– внутренние нарушители.

К внешним нарушителям могут относиться:

– спецслужбы иностранных государств (блоков государств);

– террористические, экстремистские группировки;

– разработчики, производители, поставщики программных, технических и программно-технических средств.

К внутренним нарушителям могут относиться:

– лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

– лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора;

– пользователи информационной системы;

– администраторы информационной системы и администраторы безопасности.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В качестве источников антропогенных угроз безопасности информации могут выступать:

— лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в корпоративной сети передачи данных, или нарушения функционирования корпоративной сети передачи данных или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);

— лица, имеющие доступ к корпоративной сети передачи данных, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации приведены в таблице И.1.

Таблица И.1 — Модель нарушителя

№	Вид нарушителя	Тип нарушителя	Возможные цели (мотивация) реализации угроз безопасности
1	спецслужбы иностранных государств (блоков государств)	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в ПО или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
4	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
5	Лица, обеспечивающие функционирование ИС или обслуживающие инфраструктуру оператора;	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
6	Пользователи информационной системы;	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
7	Администраторы информационной системы и администраторы безопасности.	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия

Потенциал нарушителей и их возможности представлены в таблице И.2.

Таблица И.2 — Потенциал и возможности нарушителей

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы И.2

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
3	Нарушители с высоким потенциалом	спецслужбы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

Приложение К

(обязательное)

Модель угроз безопасности информации

УТВЕРЖДЕНА

_____

(руководитель предприятия)

«___» _____ 20___ г..

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЗНАЧИМОМ ОБЪЕКТЕ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

«Корпоративной сети передачи данных»

ПРИНАДЛЕЖАЩЕЙ

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

Заречный 2020

Оглавление

Список сокращений и обозначений.. ….....1
Термины и определения.....2
Нормативно-методическое обеспечение.....3
Общие положения.....4
1 Описание корпоративной сети передачи данных….....6
1.1 Наименование ИС.....6
1.2 Назначение ИС.....6
1.3 Исходные данные об ИС.....6
2 Модель нарушителя.....8
2.1 Общие положения.....8
2.2 Внешний нарушитель.....8
2.3 Внутренний нарушитель.....8
2.4 Предположения об имеющейся у нарушителя информации об объектах реализации угроз.....9
2.5 Предположения об имеющихся у нарушителя средствах реализации угроз.....11
2.6 Источники угроз.....12
2.7 Возможные цели и потенциал нарушителей.....13
3 Перечень угроз безопасности информации.....17
4 Определение актуальных угроз.....18
4.1 Общие положения.....18
4.2 Определение уровня исходной защищённости ИС.....18
4.3 Определение вероятности реализации угроз безопасности ИС.....20
4.4 Определение возможности реализации угрозы.....20
4.5 Определение опасности угроз безопасности ИС.....21
4.6 Определение актуальности угроз безопасности.....21

Список сокращений и обозначений

КИИ - критическая информационная инфраструктура

АСУ - автоматизированная система управления

ЗОКИИ -значимый объект критической информационной инфраструктуры

ИС - информационная система

АС - автоматизированная система.

ВТСС - вспомогательные технические средства и системы.

ИБ - информационная безопасность

КЗ - контролируемая зона.

ПО - программное обеспечение.

ОС - операционная система

НСД - несанкционированный доступ.

ТС - технические средства.

BIOS - базовая система ввода-вывода.

Термины и определения

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – перечень возможных угроз информации.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической

информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Нормативно-методическое обеспечение

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами:

Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 26.03.2019) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации".

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ.

Банк данных угроз безопасности информации ФСТЭК России.

Общие положения

Настоящая модель угроз разработана в соответствии с Приказом ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

В документе устанавливаются требования к обеспечению безопасности информации в корпоративной сети передачи данных, принадлежащей АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Настоящая «Модель угроз» содержит систематизированный перечень угроз безопасности информации в корпоративной сети передачи данных, принадлежащей АО «ФНПЦ «ПО «Старт» им. М.В. Проценко». Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности информации, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз определяет актуальные угрозы для корпоративной сети передачи данных АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц корпоративной сети передачи данных, администраторов корпоративной сети передачи данных.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности корпоративной сети передачи данных от угроз безопасности информации в ходе организации и выполнения работ по обеспечению безопасности информации;
- разработка системы защиты корпоративной сети передачи данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты объектов КИИ, предусмотренных для

соответствующей категории значимости корпоративной сети передачи данных;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к корпоративной сети передачи данных.

В Модели угроз дано обобщённое описание корпоративной сети передачи данных как объекта защиты, возможных источников угроз безопасности информации, возможных видов неправомерных действий и деструктивных воздействий на корпоративную сеть передачи данных, а также основных способов их реализации.

Угрозы безопасности информации в корпоративной сети передачи данных, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности информации в корпоративной сети передачи данных. Кроме того, Модель угроз может быть пересмотрена по решению оператора (АО «ФНПЦ «ПО «Старт» им. М.В. Проценко») на основе периодически проводимых им анализа и оценки угроз безопасности информации с учетом особенностей и (или) изменений в корпоративной сети передачи данных, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности информации.

1 Описание корпоративной сети передачи данных

1.1 Наименование ИС

Корпоративная сеть передачи данных АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

1.2 Назначение ИС

Корпоративная сеть передачи данных представляет собой сеть, которая взаимодействует с распределенной сетью Госкорпорации «Росатома», объединяющая в единое информационное пространство локальные сети предприятия.

1.3 Исходные данные об ИС

Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена: система, имеющая подключения к сетям общего пользования.

Режим обработки персональных данных: многопользовательский.

Режим разграничения прав доступа пользователей системы: система с разграничением прав доступа.

Объекты защиты:

1 Защищаемая информация.

2 Технологическая информация:

- управляющая информация;
- технологическая информация средств доступа к системам управления;
- информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы;

– служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации.

3 Программно-технические средства обработки:

– общесистемное и специальное программное обеспечение (операционные системы и другие);

– резервные копии общесистемного программного обеспечения;

– инструментальные средства и утилиты систем управления ресурсами ИС;

– аппаратные средства обработки информации.

4 Средства защиты информации:

– средства управления и разграничения доступа пользователей;

– средства обеспечения регистрации и учета действий с информацией;

– средства, обеспечивающие целостность данных;

– средства антивирусной защиты.

5 Объекты и помещения, в которых размещены компоненты ИС:

Местонахождение технических средств автоматизированной системы: в пределах РФ (город Заречный, Пензенская область, пр. Мира 1).

2 Модель нарушителя

2.1 Общие положения

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

По признаку принадлежности к корпоративной сети передачи данных все нарушители делятся на две группы:

- Внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование корпоративной сети передачи данных;
- Внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование корпоративной сети передачи данных.

2.2 Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в корпоративной сети передачи данных, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам.

Предполагается, что внешний нарушитель может воздействовать на

защищаемую информацию только во время ее передачи по каналам связи.

К внешним нарушителям могут относиться:

– спецслужбы иностранных государств (блоков государств);

– террористические, экстремистские группировки;

– разработчики, производители, поставщики программных, технических и программно-технических средств.

2.3 Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа корпоративной сети передачи данных обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам корпоративной сети передачи данных в соответствии с принятой политикой информационной безопасности.

К внутренним нарушителям могут относиться:

– лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

– лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора;

– пользователи информационной системы;

– администраторы информационной системы и администраторы безопасности.

Предполагается, что возможность сговора внутренних нарушителей

маловероятна ввиду принятых организационных и контролирующих мер.

2.4 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об ИС можно выделить следующие:

- общая информация – информации о назначении и общих характеристиках ИС;
- эксплуатационная информация – информация, полученная из эксплуатационной документации;
- чувствительная информация – информация, дополняющая эксплуатационную информацию об ИС (например, сведения из проектной документации ИС).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИС;
- сведения об информационных ресурсах ИС: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (не декларированных) возможностях технических, программных и программно-технических средств ИС;
- данные о реализованных в программных средствах защиты информации принципах и алгоритмах;
- исходные тексты программного обеспечения ИС;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Степень информированности нарушителя зависит от многих факторов,

включая реализованные в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

2.5 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

– аппаратные компоненты системы защиты информации;

– доступные в свободной продаже технические средства и программное обеспечение;

– специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз информационной безопасности, а также возможности по их применению зависят от многих факторов, включая реализованные в АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой системы защиты предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства,

возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

– средств перехвата в технических каналах утечки;

– средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);

– средств воздействия на источники и через цепи питания;

– средств воздействия через цепи заземления;

– средств активного воздействия на технические средства (средств облучения).

2.6 Источники угроз

В качестве источников угроз безопасности информации могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Типы источников угроз безопасности информации:

— антропогенные источники (антропогенные угрозы);

— техногенные источники (техногенные угрозы);

— стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

— лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в корпоративной сети передачи данных, или нарушения функционирования корпоративной сети

передачи данных или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);

— лица, имеющие доступ к корпоративной сети передачи данных, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

В таблице К.1 представлены типы и виды нарушителей.

Таблица К.1 — Виды и тип нарушителя

№	Вид нарушителя	Тип нарушителя
1	спецслужбы иностранных государств (блоков государств)	Внешний
2	Террористические, экстремистские группировки	Внешний
3	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний
4	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний
5	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора;	Внутренний
6	Пользователи информационной системы;	Внутренний
7	Администраторы информационной системы и администраторы безопасности.	Внутренний

2.7 Возможные цели и потенциал нарушителей

Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации приведены в таблице К.2.

Таблица К.2 — Модель нарушителя

№	Вид нарушителя	Тип нарушителя	Возможные цели (мотивация) реализации угроз безопасности
1	спецслужбы иностранных государств (блоков государств)	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций

Продолжение таблицы К.2

№	Вид нарушителя	Тип нарушителя	Возможные цели (мотивация) реализации угроз безопасности
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
4	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
5	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора;	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
6	Пользователи информационной системы;	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
7	Администраторы информационной системы и администраторы безопасности.	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия

Потенциал нарушителей и их возможности представлены в таблице К.3.

Таблица К.3 — Потенциал и возможности нарушителей

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы К.3

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
3	Нарушители с высоким потенциалом	спецслужбы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов(микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

3 Перечень угроз безопасности информации

Под угрозами безопасности информации при их обработке в ИС понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на неё.

Система защиты информации включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности информации и информационных технологий, используемых в ИС.

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

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на ИС и её элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы ИС, вызванные деятельностью человека. Среди них, исходя их мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании ИС и её элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Для данного объекта реально существуют угрозы безопасности информации при обеспечении ее конфиденциальности, доступности, целостности.

4 Определение актуальных угроз

4.1 Общие положения

Актуальной считается угроза, которая может быть реализована в ИС и представляет опасность для защищаемой информации.

Для оценки возможности реализации угрозы применяются два показателя:

- уровень исходной защищенности ИС;
- частота (вероятность) реализации рассматриваемой угрозы.

4.2 Определение уровня исходной защищённости ИС

Под уровнем исходной защищенности ИС понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС, приведенных в таблице К.4.

Таблица К.4 — Показатель исходной защищенности ИС

Технические и эксплуатационные характеристики	Уровень защищенности		
	Высокий	Средний	Низкий
1 По территориальному размещению			
Локальная ИС, развернутая в пределах нескольких близко расположенных зданий		+	
2 По наличию соединения с сетями общего пользования:			
ИС имеющая одноточечный выход в сеть общего пользования;		+	
3 По встроенным (легальным) операциям с записями баз персональных данных:			
запись, удаление, сортировка;		+	
4 По разграничению доступа к защищаемой информации:			
ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС.		+	
5 По наличию соединений с другими базами данных иных систем:			
интегрированная ИСПДн (организация использует несколько баз данных ИС, при этом организация не является владельцем всех используемых баз данных);			+

Продолжение таблицы К.4

Технические и эксплуатационные характеристики	Уровень защищенности		
6 По уровню обобщения (обезличивания) информации:			
ИС, в которой предоставленные данные пользователю не являются обезличенными;			+
7 По объему информации. Которая предоставляется сторонним пользователям без предварительной обработки:			
ИС, предоставляющая часть информации.		+	

Исходная степень защищенности определяется следующим образом:

– ИС имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИС соответствует уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – по среднему уровню защищенности (положительные решения по второму столбцу);

– ИС имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИС соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – к низкому уровню защищенности;

– ИС имеет низкую степень защищенности, если не выполняются условия по пунктам 1 и 2.

Согласно таблице К.3, пять характеристик ИС (71,4%) соответствуют среднему уровню защищенности, две характеристики ИС (28,56%) – низкому. Следовательно, ИС имеет средний уровень исходной защищенности.

При составлении перечня актуальных угроз безопасности информации, каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y1, а именно:

– 0 для высокой степени исходной защищенности;

– 5 для средней степени исходной защищенности;

– 10 для низкой степени исходной защищенности.

Числовой коэффициент уровня исходной защищенности ИС Y1 равно 5.

4.3 Определение вероятности реализации угроз безопасности ИС

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для данной ИС в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;

– низкая вероятность – объективные предпосылки для осуществления угрозы существуют, но принятые меры существенно затрудняют ее реализацию;

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны;

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности информации не приняты.

При составлении перечня актуальных угроз безопасности информации каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

– 0 для маловероятной угрозы;

– 2 для низкой вероятности угрозы;

– 5 для средней вероятности угрозы;

– 10 для высокой вероятности угрозы.

Данные о вероятности реализации угроз безопасности информации, обрабатываемой в ИС, представлены в таблице К.3.

4.4 Определение возможности реализации угрозы

Возможность реализации угрозы определяется коэффициентом реализуемости угрозы Y, значение которого определяется соотношением:

$$Y = (Y1 + Y2)/20 \quad (1)$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если Y больше 0, но меньше 0,3, то возможность реализации угрозы признается низкой;
- если Y больше 0,3, но меньше 0,6, то возможность реализации угрозы признается средней;
- если Y больше 0,6, но меньше 0,8, то возможность реализации угрозы признается высокой;
- если Y больше 0,8, то возможность реализации угрозы признается очень высокой.

Данные о возможности реализации угроз безопасности информации, обрабатываемой в ИС, представлены в таблице К.7.

4.5 Определение опасности угроз безопасности ИС.

При оценке опасности угрозы определяется вербальный показатель опасности для ИС. Этот показатель имеет три значения:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям;
- средняя опасность – если реализация угрозы может привести к негативным последствиям;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям.

Данные по оценке опасности угроз безопасности информации, обрабатываемой в ИС, представлены в таблице К.7.

4.6 Определение актуальности угроз безопасности.

Определение актуальности угроз безопасности информации, проводится в соответствии с правилами, приведенными в таблице К.6.

Таблица К.6 – Правила отнесения угроз безопасности информации к актуальным

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

Данные по оценке актуальности угроз безопасности информации, обрабатываемой в ИС, представлены в таблице К.7.

Таблица К.7 — Данные по оценке актуальности угроз безопасности информации

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
			Вероятность (частота) реализации угрозы	Обоснование	Вероятность возникновения угрозы (Y2)				
1	Угроза автоматического распространения вредоносного кода в грид-системе УБИ.001								Технология не применяется в данной ИС
2	Угроза агрегирования данных, передаваемых в грид-системе УБИ.002								Технология не применяется в данной ИС
3	Угроза анализа криптографических алгоритмов и их реализации УБИ. 003	5	маловероятно	На создаваемом АП отсутствует криптографическое ПО. Отсутствие у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	0	0,25	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
4	Угроза аппаратного сброса пароля BIOS УБИ. 004	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
5	Угроза внедрения вредоносного кода в BIOS УБИ. 005	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	2	0,35	Низкая	Низкая	Неактуальная
6	Угроза внедрения кода или данных УБИ.006	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами	2	0,35	Низкая	Низкая	Неактуальная
7	Угроза воздействия на программы с высокими привилегиями УБИ. 007	5	низкая	Отсутствие административных привилегий у пользователя Наличие доверенного канала связи посредством СКЗИ. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
8	Угроза восстановления аутентификационной информации УБИ. 008	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
9	Угроза восстановления предыдущей уязвимой версии BIOS УБИ. 009	5	низкая	На АП установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
10	Угроза выхода процесса за пределы виртуальной машины УБИ.010								Данная угроза не применяется к рассматриваемой ИС
11	Угроза деавторизации санкционированного клиента беспроводной сети УБИ.011								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
12	Угроза деструктивного изменения конфигурации/среды окружения программ УБИ.012	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
13	Угроза деструктивного использования декларированного функционала BIOS УБИ.013	5	низкая	На АП установлена версия BIOS/UEFI, для которой на момент её работы известны уязвимости.	2	0,35	Низкая	Низкая	Неактуальная
14	Угроза длительного удержания вычислительных ресурсов пользователями УБИ.014	5	низкая	Использование на АП базового проверенного набора ПО. Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
15	Угроза доступа к защищаемым файлам с использованием обходного пути УБИ.015	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
16	Угроза доступа к локальным файлам сервера при помощи URL УБИ.016	5	низкая	Отсутствие у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	2	0,35	Низкая	Низкая	Неактуальная
17	Угроза доступа/перехвата/изменения HTTP cookies УБИ.017	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к защищаемой информации	5	0,5	Средняя	Средняя	Актуальная
18	Угроза загрузки нештатной операционной системы УБИ.018	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	Низкая	Низкая	Неактуальная
19	Угроза заражения DNS-кеша УБИ.019	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
20	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг УБИ.20								Технология не применяется в данной ИС
21	Угроза злоупотребления доверием потребителей облачных услуг УБИ.21								Технология не применяется в данной ИС
22	Угроза избыточного выделения оперативной памяти УБИ.022	5	низкая	Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО. Возможность выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
23	Угроза изменения компонентов информационной (автоматизированной) системы УБИ.023	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
24	Угроза изменения режимов работы аппаратных элементов компьютера УБИ.024	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
25	Угроза изменения системных и глобальных переменных УБИ.025	5	низкая	Отсутствие возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
26	Угроза искажения XML-схемы УБИ.026	5	средняя	Наличие доверенного канала связи посредством СКЗИ Возможность изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером.	5	0,5	Средняя	Средняя	Актуальная
27	Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027	5	средняя	Возможность дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
28	Угроза использования альтернативных путей доступа к ресурсам УБИ.028	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).	5	0,5	Средняя	Средняя	Актуальная
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами УБИ.029								Технология не применяется в данной ИС
30	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию УБИ.030	5	средняя	Наличие у нарушителя сведений о производителе/модели объекта защиты (ОЗ) и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для ОЗ;	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
31	Угроза использования механизмов авторизации для повышения привилегий УБИ.031	5	средняя	Возможность получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа	5	0,5	Средняя	Средняя	Актуальная
32	Угроза использования поддельных цифровых подписей BIOS УБИ.032	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
33	Угроза использования слабостей кодирования входных данных УБИ.033	5	низкая	Возможность осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.).	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
34	Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034	5	средняя	Возможность осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Наличие доверенного канала связи посредством СКЗИ	5	0,5	Средняя	Средняя	Актуальная
35	Угроза использования слабых криптографических алгоритмов BIOS УБИ.035	5	низкая	Сложность использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI.	2	0,35	Низкая	Низкая	Неактуальная
36	Угроза исследования механизмов работы программы УБИ.036	5	низкая	Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
37	Угроза исследования приложения через отчёты об ошибках УБИ.037	5	низкая	Отсутствие у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	2	0,35	Низкая	Низкая	Неактуальная
38	Угроза исчерпания вычислительных ресурсов хранилища больших данных УБИ.038								Технология не применяется в данной ИС
39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS УБИ.039	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя	2	0,35	Низкая	Низкая	Неактуальная
40	Угроза конфликта юрисдикций различных стран УБИ.40								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
41	Угроза межсайтового скриптинга УБИ.041								Технология не применяется в данной ИС
42	Угроза межсайтовой подделки запроса УБИ.042								Данная угроза не применяется к рассматри-ваемой ИС
43	Угроза нарушения доступности облачного сервера УБИ.043								Технология не применяется в данной ИС
44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины УБИ.044								Данная угроза не применяется к рассматри-ваемой ИС
45	Угроза нарушения изоляции среды исполнения BIOS УБИ.045	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия УБИ.046								Данная угроза не применяется к рассматриваемой ИС
47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке УБИ.047								Технология не применяется в данной ИС
48	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин УБИ.048								Данная угроза не применяется к рассматриваемой ИС
49	Угроза нарушения целостности данных кеша УБИ.049	5	низкая	Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных УБИ.050								Технология не применяется в данной ИС
51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания УБИ.051	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения УБИ.052								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
53	Угроза невозможности управления правами пользователей BIOS УБИ.053	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
54	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг УБИ.054								Технология не применяется в данной ИС
55	Угроза незащищённого администрирования облачных услуг УБИ.055								Технология не применяется в данной ИС
56	Угроза некачественного переноса инфраструктуры в облако УБИ.056								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
57	Угроза неконтролируемого копирования данных внутри хранилища больших данных УБИ.057								Технология не применяется в данной ИС
58	Угроза неконтролируемого роста числа виртуальных машин УБИ.058								Технология не применяется в данной ИС
59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов УБИ.059								Технология не применяется в данной ИС
60	Угроза неконтролируемого уничтожения информации хранилищем больших данных УБИ.060								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
61	Угроза некорректного задания структуры данных транзакции УБИ.061	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС, реализация.	2	0,35	Низкая	Низкая	Неактуальная
62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера УБИ.062								Данная угроза не применяется к рассматриваемой ИС
63	Угроза некорректного использования функционала программного и аппаратного обеспечения УБИ.063	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя	2	0,35	Низкая	Низкая	Неактуальная
64	Угроза некорректной реализации политики лицензирования в облаке УБИ.064								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
65	Угроза неопределённости в распределении ответственности между ролями в облаке УБИ.065								Технология не применяется в данной ИС
66	Угроза неопределённости ответственности за обеспечение безопасности облака УБИ.066								Технология не применяется в данной ИС
67	Угроза неправомерного ознакомления с защищаемой информацией УБИ.067	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
68	Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением УБИ.068	5	средняя	Отсутствие возможность осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
69	Угроза неправомерных действий в каналах связи УБИ.069	5	средняя	Возможность несанкционированного доступа к сетевому трафику у нарушителя	5	0,5	Средняя	Средняя	Актуальная
70	Угроза непрерывной модернизации облачной инфраструктуры УБИ.070								Технология не применяется в данной ИС
71	Угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071	5	средняя	Удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных; Технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; Информация не хранится в криптографически преобразованном виде	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Число-вой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS УБИ.072	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети УБИ.073								Технология не применяется в данной ИС
74	Угроза несанкционированного доступа к аутентификационной информации УБИ.074	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС АС.	2	0,35	низкая	низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
75	Угроза несанкционированного доступа к виртуальным каналам передачи УБИ.075								Технология не применяется в данной ИС
76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети УБИ.076								Технология не применяется в данной ИС
77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение УБИ.077								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети УБИ.078								Технология не применяется в данной ИС
79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин УБИ.079								Технология не применяется в данной ИС
80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети УБИ.080								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
81	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы УБИ.081								Технология не применяется в данной ИС
82	Угроза несанкционированного доступа к сегментам вычислительного поля УБИ.082								Данная угроза не применяется к рассматриваемой ИС
83	Угроза несанкционированного доступа к системе по беспроводным каналам УБИ.083								Данная угроза не применяется к рассматриваемой ИС
84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети УБИ.084								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации УБИ.085								Технология не применяется в данной ИС
86	Угроза несанкционированного изменения аутентификационной информации УБИ.086	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
87	Угроза несанкционированного использования привилегированных функций BIOS УБИ.087	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
88	Угроза несанкционированного копирования защищаемой информации УБИ.088	5	средняя	Контроль со стороны ответственных за эксплуатацию ТС ИС. Возможность неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).	5	0,5	Средняя	Средняя	Актуальная
89	Угроза несанкционированного редактирования реестра УБИ.089	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
90	Угроза несанкционированного создания учётной записи пользователя УБИ.090	5	низкая	Отсутствие прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	2	0,35	Низкая	Низкая	Неактуальная
91	Угроза несанкционированного удаления защищаемой информации УБИ.091	5	низкая	Использование на АП базового проверенного набора ПО. Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам УБИ.092								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
93	Угроза несанкционированного управления буфером УБИ.093	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
94	Угроза несанкционированного управления синхронизацией и состоянием УБИ.094	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации. Возможность изменения нарушителем последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния ИС, или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.).	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
95	Угроза несанкционированного управления указателями УБИ.095	5	низкая	Предоставление прав доступа к информационным ресурсам информационной системы по принципу минимальной достаточности.	2	0,35	Низкая	Низкая	Неактуальная
96	Угроза несогласованности политик безопасности элементов облачной инфраструктуры УБИ.096								Технология не применяется в данной ИС
97	Угроза несогласованности правил доступа к большим данным УБИ.097	5	низкая	Использования политик безопасности, согласованных между собой.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098	5	средняя	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика. Возможность определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов.	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
99	Угроза обнаружения хостов УБИ.099	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика. Сканирование нарушителем вычислительной сети для выявления работающих сетевых узлов.	2	0,35	Низкая	Низкая	Неактуальная
100	Угроза обхода некорректно настроенных механизмов аутентификации УБИ.100	5	низкая	Наличие корректных значений параметров настройки механизмов аутентификации и авторизации.	2	0,35	Низкая	Низкая	Неактуальная
101	Угроза общедоступности облачной инфраструктуры УБИ.101								Технология не применяется в данной ИС
102	Угроза опосредованного управления группой программ через совместно используемые данные УБИ.102	5	низкая	Возможность опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные и др.)	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
103	Угроза определения типов объектов защиты УБИ.103	5	низкая	Отсутствие средств межсетевого экранирования и фильтрации сетевого трафика.	2	0,35	Низкая	Низкая	Неактуальная
104	Угроза определения топологии вычислительной сети УБИ.104	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Возможность определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.	2	0,35	Низкая	Низкая	Неактуальная
105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных УБИ.105								Технология не применяется в данной ИС
106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера УБИ.106								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
107	Угроза отключения контрольных датчиков УБИ.107								Данная угроза не применяется к рассматриваемой ИС
108	Угроза ошибки обновления гипервизора УБИ.108								Технология не применяется в данной ИС
109	Угроза перебора всех настроек и параметров приложения УБИ.109	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Возможность получения нарушителем доступа к дополнительному скрытому функционалу или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
110	Угроза перегрузки грид-системы вычислительными заданиями УБИ.110								Технология не применяется в данной ИС
111	Угроза передачи данных по скрытым каналам УБИ.111								Данная угроза не применяется к рассматриваемой ИС
112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением УБИ.112								Данная угроза не применяется к рассматриваемой ИС
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники УБИ.113	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
114	Угроза переполнения целочисленных переменных УБИ.114	5	низкая	Отсутствие у внешнего нарушителя сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных. Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации УБИ.115	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Отсутствие у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	2	0,35	Низкая	Низкая	Неактуальная
116	Угроза перехвата данных, передаваемых по вычислительной сети УБИ.116	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
117	Угроза перехвата привилегированного потока УБИ.117	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
118	Угроза перехвата привилегированного процесса УБИ.118	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
119	Угроза перехвата управления гипервизором УБИ.119								Технология не применяется в данной ИС
120	Угроза перехвата управления средой виртуализации УБИ.120								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
121	Угроза повреждения системного реестра УБИ.121	5	низкая	Возникновение ошибок в работе отдельных процессов или всей операционной системы. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
122	Угроза повышения привилегий УБИ.122	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
123	Угроза подбора пароля BIOS УБИ.123	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
124	Угроза подделки записей журнала регистрации событий УБИ.124	5	низкая	Технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
125	Угроза подключения к беспроводной сети в обход процедуры аутентификации УБИ.125								Данная угроза не применяется к рассматриваемой ИС
126	Угроза подмены беспроводного клиента или точки доступа УБИ.126								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
127	Угроза подмены действия пользователя путём обмана УБИ.127	5	низкая	Применение методов борьбы с социальной инженерией. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
128	Угроза подмены доверенного пользователя УБИ.128	5	низкая	Возможность нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Наличие доверенного канала связи посредством СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
129	Угроза подмены резервной копии программного обеспечения BIOS УБИ.129	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Отсутствие возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии ПО BIOS/UEFI, предварительно подменённой нарушителем.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
130	Угроза подмены содержимого сетевых ресурсов УБИ.130								Данная угроза не применяется к рассматриваемой ИС
131	Угроза подмены субъекта сетевого доступа УБИ.131								Данная угроза не применяется к рассматриваемой ИС
132	Угроза получения предварительной информации об объекте защиты УБИ.132								Данная угроза не применяется к рассматриваемой ИС
133	Угроза получения сведений о владельце беспроводного устройства УБИ.133								Технология не применяется в данной ИС
134	Угроза потери доверия к поставщику облачных услуг УБИ.134								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасности угрозы	Актуальность угрозы
135	Угроза потери и утечки данных, обрабатываемых в облаке УБИ.135								Технология не применяется в данной ИС
136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных УБИ.136								Технология не применяется в данной ИС
137	Угроза потери управления облачными ресурсами УБИ.137								Технология не применяется в данной ИС
138	Угроза потери управления собственной инфраструктурой при переносе её в облако УБИ.138								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
139	Угроза преодоления физической защиты УБИ.139	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Контроль физического доступа (наличие замков в помещении, обученный проинструктированный персонал и т.п.). Отсутствие возможности любого из методов проникновения на объект	2	0,35	Низкая	Низкая	Неактуальная
140	Угроза приведения системы в состояние «отказ в обслуживании» УБИ.140	5	низкая	Возможность отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов.	2	0,35	Низкая	Низкая	Неактуальная
141	Угроза привязки к поставщику облачных услуг УБИ.141								Технология не применяется в данной ИС
142	Угроза приостановки оказания облачных услуг вследствие технических сбоев УБИ.142								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.143	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
144	Угроза программного сброса пароля BIOS УБИ.144	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС. Отсутствие в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля	2	0,35	Низкая	Низкая	Неактуальная
145	Угроза пропуска проверки целостности программного обеспечения УБИ.145	5	низкая	Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера УБИ.146								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
147	Угроза распространения несанкционированно повышенных прав на всю грид-систему УБИ.147								Технология не применяется в данной ИС
148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных УБИ.148								Технология не применяется в данной ИС
149	Угроза сбоя обработки специальным образом изменённых файлов УБИ.149	5	низкая	Отсутствие у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке;	2	0,35	Низкая	Низкая	Неактуальная
150	Угроза сбоя процесса обновления BIOS УБИ.150	5	низкая	Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL УБИ.151	5	низкая	Наличие доверенного канала связи посредством СКЗИ. Возможность получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера.	2	0,35	Низкая	Низкая	Неактуальная
152	Угроза удаления аутентификационной информации УБИ.152	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя.	2	0,35	Низкая	Низкая	Неактуальная
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов УБИ.153	5	низкая	Отсутствие у нарушителя сведений о сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов. Отсутствие у нарушителя сведений о сетевом адресе дискредитируемой системы.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS УБИ.154	5	низкая	Установка и использование проверенного ПО. Обслуживание и ремонт компьютера осуществляется доверенными специалистами.	2	0,35	Низкая	Низкая	Неактуальная
155	Угроза утраты вычислительных ресурсов УБИ.155	5	низкая	Отсутствие у нарушителя сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы	2	0,35	Низкая	Низкая	Неактуальная
156	Угроза утраты носителей информации УБИ.156	5	низкая	Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опасно-сти угрозы	Актуальность угрозы
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.157	5	низкая	Отсутствие возможности получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.) Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
158	Угроза форматирования носителей информации УБИ.158	5	низкая	Создание резервных копий информации, хранящейся на носителях.	2	0,35	Низкая	Низкая	Неактуальная
159	Угроза «форсированного веб-браузинга» УБИ.159								

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.160	5	низкая	Отсутствие у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации. Контроль со стороны ответственных за эксплуатацию ТС ИС.	2	0,35	Низкая	Низкая	Неактуальная
161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями УБИ.161								Технология не применяется в данной ИС
162	Угроза эксплуатации цифровой подписи программного кода УБИ.162	5	низкая	В системах не используются цифровые подписи кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма прописывания программного кода	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
163	Угроза перехвата исключения/сигнала из привилегированного блока функций УБИ.163	5	низкая	Предоставление прав доступа к информационным ресурсам ИС по принципу минимальной достаточности. Отсутствие административных привилегий у пользователя. Использование на АП базового проверенного набора ПО.	2	0,35	Низкая	Низкая	Неактуальная
164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре УБИ.164								Технология не применяется в данной ИС
165	Угроза включения в проект не достоверно испытанных компонентов УБИ.165	5	низкая	Для применения в системе выбираются компоненты в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Использование сертифицированного ПО.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
166	Угроза внедрения системной избыточности УБИ.166	5	низкая	Отсутствие избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект) программного обеспечения (или системы в целом).	2	0,35	Низкая	Низкая	Неактуальная
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов УБИ.167								Данная угроза не применяется к рассматриваемой ИС
168	Угроза «кражи» учётной записи доступа к сетевым сервисам УБИ.168								Данная угроза не применяется к рассматриваемой ИС
169	Угроза наличия механизмов разработчика УБИ.169	5	низкая	Использование проверенного ПО, не подразумевающего использования отладочных механизмов	2	0,35	Низкая	Низкая	Неактуальная
170	Угроза неправомерного шифрования информации УБИ.170	5	низкая	Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
171	Угроза скрытного включения вычислительного устройства в состав бот-сети УБИ.171								Технология не применяется в данной ИС
172	Угроза распространения «почтовых червей» УБИ.172								Данная угроза не применяется к рассматриваемой ИС
173	Угроза «спама» веб-сервера УБИ.173								Данная угроза не применяется к рассматриваемой ИС
174	Угроза «фарминга» УБИ.174								Данная угроза не применяется к рассматриваемой ИС
175	Угроза «фишинга» УБИ.175								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опаснос-ти угрозы	Актуальность угрозы
176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты УБИ.176	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью УБИ.177	5	низкая	Отсутствие (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора» Предоставление прав пользователю в минимально достаточном объем.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
178	Угроза несанкционированного использования системных и сетевых утилит УБИ.178	5	низкая	Предоставление прав пользователю в минимально достаточном объем. Отсутствие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему, предназначенных для использования администратором для диагностики и обслуживания системы	2	0,35	Низкая	Низкая	Неактуальная
179	Угроза несанкционированной модификации защищаемой информации УБИ.179	5	низкая	Предоставление прав пользователю в минимально достаточном объеме. Контроль со стороны ответственных за эксплуатацию ТС ИС. Использование доверенно-го канала связи СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
180	Угроза отказа подсистемы обеспечения температурного режима УБИ.180	5	низкая	Реализация угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опаснос-ти угрозы	Актуальность угрозы
181	Угроза перехвата одноразовых паролей в режиме реального времени УБИ.181	5	низкая	Отсутствие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия Невозможность осуществления нарушителем перехвата трафика между системой и пользователем, ввиду использования доверенного канала связи СКЗИ	2	0,35	Низкая	Низкая	Неактуальная
182	Угроза физического устаревания аппаратных компонентов УБИ.182	5	низкая	Возможность нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций).	5	0,5	Средняя	Средняя	Актуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэф-фициент исходной защищен-ности (Y1)	Частота (вероятность) реализации угрозы			Коэффи-циент реализуе-мости угрозы (Y)	Вербаль-ная интерпре-тация реализуе-мости угрозы	Вербаль-ный показа-тель опаснос-ти угрозы	Актуальность угрозы
183	Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.183								Данная угроза не применяется к рассматри-ваемой ИС
184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства УБИ.184								Технология не применяется в данной ИС
185	Угроза несанкционированного изменения параметров настройки средств защиты информации УБИ.185	5	низкая	Отсутствие СЗИ, вследствие этого отсутствие у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	2	0,35	Низкая	Низкая	Неактуальная
186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент УБИ.186								Данная угроза не применяется к рассматри-ваемой ИС
187	Угроза несанкционированного воздействия на средство защиты информации УБИ.187	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
188	Угроза подмены программного обеспечения УБИ.188								Данная угроза не применяется к рассматриваемой ИС
189	Угроза маскирования действий вредоносного кода УБИ.189	5	низкая	На АП отсутствуют СЗИ от НСД.	2	0,35	Низкая	Низкая	Неактуальная
190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет УБИ.190								Данная угроза не применяется к рассматриваемой ИС
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения УБИ.191	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объем	2	0,35	Низкая	Низкая	Неактуальная
192	Угроза использования уязвимых версий программного обеспечения УБИ.192	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объем	2	0,35	Низкая	Низкая	Неактуальная

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика УБИ.193	5	низкая	Использование на АП базового проверенного набора ПО. Наличие доверенного канала связи посредством СКЗИ.	2	0,35	Низкая	Низкая	Неактуальная
194	Угроза несанкционированного использования привилегированных функций мобильного устройства УБИ.194								Технология не применяется в данной ИС
195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы УБИ.195								Данная угроза не применяется к рассматриваемой ИС
196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве УБИ.196								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
197	Угроза хищения аутентификационной информации из временных файлов cookie УБИ.197	5	низкая	Использование на АП базового проверенного набора ПО. На АП закрыт RDP-порт.	2	0,35	Низкая	Низкая	Неактуальная
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов УБИ.198	5	низкая	Использование на АП базового проверенного набора ПО. Предоставление прав пользователю в минимально достаточном объем На АП закрыт RDP-порт.	2	0,35	Низкая	Низкая	Неактуальная
199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.199								Технология не применяется в данной ИС
200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов УБИ.200								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере УБИ.201	5	низкая	Использование защищенного канала связи СКЗИ Настройка браузера в режиме, в котором не активирована функция автоматического заполнения форм авторизации	2	0,35	Низкая	Низкая	Неактуальная
202	Угроза несанкционированной установки приложений на мобильные устройства УБИ.202								Технология не применяется в данной ИС
203	Угроза утечки информации с неподключенных к сети Интернет компьютеров УБИ.203								Данная угроза не применяется к рассматриваемой ИС
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров УБИ.204								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты УБИ.205	5	низкая	Возможность нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов.	2	0,35	Низкая	Низкая	Неактуальная
206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем УБИ.206								Данная угроза не применяется к рассматриваемой ИС
207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей) УБИ.207								Данная угроза не применяется к рассматриваемой ИС
208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники УБИ.208								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора УБИ.209								Данная угроза не применяется к рассматриваемой ИС
210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения УБИ.210								Данная угроза не применяется к рассматриваемой ИС
211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем УБИ.211								Данная угроза не применяется к рассматриваемой ИС
212	Угроза перехвата управления информационной системой УБИ.212								Данная угроза не применяется к рассматриваемой ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
213	Угроза обхода многофакторной аутентификации УБИ.213								Данная угроза не применяется к рассматриваемой ИС
214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации УБИ.214								Данная угроза не применяется к рассматриваемой ИС
215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов УБИ.215								Данная угроза не применяется к рассматриваемой ИС
216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах УБИ.216								Технология не применяется в данной ИС

Продолжение таблицы К.7

№	Угрозы безопасности информации	Числовой коэффициент исходной защищенности (Y1)	Частота (вероятность) реализации угрозы			Коэффициент реализуемости угрозы (Y)	Вербальная интерпретация реализуемости угрозы	Вербальный показатель опасности угрозы	Актуальность угрозы
217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения УБИ.217								Данная угроза не применяется к рассматриваемой ИС

Исходя из результатов определения актуальности угроз, содержащихся в таблице К.7, для ИС актуальными являются следующие угрозы:

– угроза доступа/перехвата/изменения HTTP cookies УБИ.017;

– угроза искажения XML-схемы УБИ.026;

– угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027;

– угроза использования альтернативных путей доступа к ресурсам УБИ.028;

– угроза использования информации идентификации/аутентификации, заданной по умолчанию УБИ.030;

– угроза использования механизмов авторизации для повышения привилегий УБИ.031;

– угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034;

– угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.068;

– угроза неправомерных действий в каналах связи УБИ.069;

– угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071;

– угроза несанкционированного копирования защищаемой информации УБИ.088;

– угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098;

– угроза физического устаревания аппаратных компонентов УБИ.182.

Описание актуальных угроз безопасности приведено в таблице К.8.

Таблица К.8 — Описание актуальных угроз безопасности информации

№	Угрозы безопасности	Источник угроз	Уязвимости	Сценарии	Последствия
1	Угроза доступа/перехвата/ изменения HTTP cookies УБИ.017	Внешний нарушитель с низким потенциалом	BDU:2018-00868: Уязвимость браузера Firefox, связанная с ошибками реализации хранилища файлов cookies, позволяющая нарушителю получить доступ к файлам cookies httpOnly	Несанкционированный доступ к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя)	Нарушение конфиден-циальности и доступности
2	Угроза искажения XML-схемы УБИ.026	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	BDU:2020-00402: Уязвимость компонента XML Parsing XML-редактора Easy XML Editor, позволяющая нарушителю вызвать отказ в обслуживании приложения или осуществить чтение произвольных файлов в системе	Изменение нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером.	Нарушение целостности и доступности
3	Угроза искажения вводимой и выводимой на периферийные устройства информации УБИ.027	Внутренний нарушитель с низким потенциалом Внешний нарушитель с высоким потенциалом	BDU:2020-02177: Уязвимость компонента Microsoft Windows Graphics операционных систем Windows, позволяющая нарушителю получить несанкционированный доступ к защищаемой информации	Дезинформирование пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации; подмена или искажение информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства	Нарушение целостности

Продолжение таблицы К.8

№	Угрозы безопасности	Источник угроз	Уязвимости	Сценарии	Последствия
4	Угроза использования альтернативных путей доступа к ресурсам УБИ.028	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2020-02199: Уязвимость службы Work Folder Service операционных систем Windows, позволяющая нарушителю повысить свои привилегии	Несанкционированный доступ к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса)	Нарушение конфиден-циальности
5	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию УБИ.030	Внутренний нарушитель с низким потенциалом Внешний нарушитель со средним потенциалом	BDU:2017-02221: Уязвимость микропрограммного обеспечения маршрутизатора Axesstel MU553S, связанная с использованием по умолчанию стандартного пароля для учётной записи администратора, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность данных	Прохождение нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты	Нарушение конфиден-циальности, целостности и доступности
6	Угроза использования механизмов авторизации для повышения привилегий УБИ.031	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2019-01295: Уязвимость системы управления базами данных PostgreSQL, связанная с ошибками авторизации, позволяющая нарушителю повысить свои привилегии	Получение доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа	Нарушение конфиден-циальности

Продолжение таблицы К.8

№	Угрозы безопасности	Источник у	Уязвимости	Сценарии	Последствия
7	Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.034	Внешний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2019-03486: Уязвимость реализации сетевого протокола Microsoft Server Message Block (SMB) операционных систем Windows, позволяющая нарушителю раскрыть защищаемую информацию	Несанкционированный доступ к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов	Нарушение конфиден-циальности,целостности и доступности
8	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением УБИ.068	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	BDU:2019-04302: Уязвимость компонента API браузера Firefox, позволяющая нарушителю подменить пользовательский интерфейс	Осуществление нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API).	Нарушение конфиден-циальности, целостности и доступности
9	Угроза неправомерных действий в каналах связи УБИ.069	Внешний нарушитель с низким потенциалом	BDU:2017-01098: Уязвимость протокола SMBv1 операционной системы Microsoft Windows, позволяющая нарушителю выполнить произвольный код	Внесение нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи	Нарушение конфиден-циальности и целостности
10	Угроза несанкционированного восстановления удалённой защищаемой информации УБИ.071	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2020-02196: Уязвимость драйвера базы данных Microsoft JET Database Engine операционных систем Windows, позволяющая нарушителю выполнить произвольный код	Осуществление прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации	Нарушение конфиден-циальности

Продолжение таблицы К.8

№	Угрозы безопасности	Источник угроз	Уязвимости	Сценарии	Последствия
11	Угроза несанкционированного копирования защищаемой информации УБИ.088	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	BDU:2020-01826: Уязвимость браузера Firefox, связанная с неправильным назначением прав доступа для критического ресурса, позволяющая нарушителю получить несанкционированный доступ к информации	Неправомерное получение нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы	Нарушение конфиденциальности
12	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб УБИ.098	Внешний нарушитель с низким потенциалом	BDU:2017-01328: Уязвимость операционной системы Windows, позволяющая нарушителю выполнить произвольный код	Определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов	Нарушение конфиденциальности
13	Угроза физического устаревания аппаратных компонентов УБИ.182	Внутренний нарушитель с низким потенциалом	Чувствительность к влажности, пыли, загрязнению	Нарушение функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания, обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций).	Нарушение доступности

Приложение Л

(обязательное)

Базовый набор мер по обеспечению безопасности значимого объекта для III категории значимости

Базовый набор мер по обеспечению безопасности значимого объекта для III категории значимости представлен в таблице Л.1.

Таблица Л.1— Базовый набор мер

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
		3
I. Идентификация и аутентификация (ИАФ)		
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+
ИАФ.2	Идентификация и аутентификация устройств	+
ИАФ.3	Управление идентификаторами	+
ИАФ.4	Управление средствами аутентификации	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+
ИАФ.7	Защита аутентификационной информации при передаче	+
II. Управление доступом (УПД)		
УПД.0	Регламентация правил и процедур управления доступом	+
УПД.1	Управление учетными записями пользователей	+
УПД.2	Реализация модели управления доступом	+
УПД.4	Разделение полномочий (ролей) пользователей	+
УПД.5	Назначение минимально необходимых прав и привилегий	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+

Продолжение таблицы Л.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+
УПД.13	Реализация защищенного удаленного доступа	+
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+
ЗНИ.1	Учет машинных носителей информации	+
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+
V. Аудит безопасности (АУД)		
АУД.0	Регламентация правил и процедур аудита безопасности	+
АУД.1	Инвентаризация информационных ресурсов	+
АУД.2	Анализ уязвимостей и их устранение	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+
АУД.4	Регистрация событий безопасности	+
АУД.6	Защита информации о событиях безопасности	+
АУД.7	Мониторинг безопасности	+

Продолжение таблицы Л.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
АУД.8	Реагирование на сбои при регистрации событий безопасности	+
АУД.10	Проведение внутренних аудитов	+
VI. Антивирусная защита (АВЗ)		
АВЗ.0	Регламентация правил и процедур антивирусной защиты	+
АВЗ.1	Реализация антивирусной защиты	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+
VIII. Обеспечение целостности (ОЦЛ)		
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+
ОЦЛ.1	Контроль целостности программного обеспечения	+
IX. Обеспечение доступности (ОДТ)		
ОДТ.0	Регламентация правил и процедур обеспечения доступности	+
ОДТ.4	Резервное копирование информации	+
ОДТ.5	Обеспечение возможности восстановления информации	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+
X. Защита технических средств (ЗТС)		
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+
ЗТС.2	Организация контролируемой зоны	+
ЗТС.3	Управление физическим доступом	+

Продолжение таблицы Л.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+
ЗТС.5	Защита от внешних воздействий	+
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)		
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+
ЗИС.5	Организация демилитаризованной зоны	+
ЗИС.6	Управление сетевыми потоками	+
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+
ЗИС.19	Защита информации при ее передаче по каналам связи	+
ЗИС.20	Обеспечение доверенных канала, маршрута	+
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+
ЗИС.32	Защита беспроводных соединений	+
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+
ЗИС.35	Управление сетевыми соединениями	+
ЗИС.38	Защита информации при использовании мобильных устройств	+

Продолжение таблицы Л.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+
XII. Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+
ИНЦ.1	Выявление компьютерных инцидентов	+
ИНЦ.2	Информирование о компьютерных инцидентах	+
ИНЦ.3	Анализ компьютерных инцидентов	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+
XIII. Управление конфигурацией (УКФ)		
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+
УКФ.2	Управление изменениями	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+
XIV. Управление обновлениями программного обеспечения (ОПО)		
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+
ОПО.3	Тестирование обновлений программного обеспечения	+
ОПО.4	Установка обновлений программного обеспечения	+

Продолжение таблицы Л.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)		
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+
ДНС.1	Разработка плана действий в нештатных ситуациях	+
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+
XVII. Информирование и обучение персонала (ИПО)		
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+
ИПО.2	Обучение персонала правилам безопасной работы	+
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+

Приложение М

(обязательное)

Техническое задание на создание системы безопасности значимого объекта критической информационной инфраструктуры

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

№_____

СОГЛАСОВАНО	УТВЕРЖДАЮ
Должность	Должность
_____Фамилия И.О.	_____Фамилия И.О.
«___» _____ 20__ г.	«___» _____ 20__ г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на создание системы безопасности значимого объекта КИИ «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

Заречный 2020

Содержание

Список сокращений и обозначений.. ….....1
Термины и определения.....2
1 Общие положения.....3
2 Цели и задачи создания системы 3
3 Категория значимости.....3
4 Перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать ЗОКИИ.....4
5 Перечень типов объектов защиты значимого объекта.....4
6 Требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта.....5
7 Этапы работ создания системы безопасности значимого объекта.....6
8 Требования к применяемым программным и программно-аппаратным средствам.....7
9 Требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре).....8
10 Требования к информационному взаимодействию значимого объекта с иными объектами КИИ, а также иными ИС, АСУ или ИТКС.....8
11 Состав и содержание мер по обеспечению безопасности КИИ.....9

Список сокращений и обозначений

ИС – информационная система.

АСУ — автоматизированная система управления.

ИТКС — информационно телекоммуникационная система.

КИИ — критическая информационная инфраструктура.

КЗ – контролируемая зона.

МЭ – межсетевой экран.

НСД – несанкционированный доступ.

ПО – программное обеспечение.

ПЭВМ – персональная электронно-вычислительная машина.

СВТ – средство вычислительной техники.

СОИБ ЗО – система обеспечения безопасности значимого объекта.

ТС – технические средства.

Термины и определения

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством.

Накопитель информации – устройство, предназначенное для записи и (или) чтения информации на носитель информации. Накопитель информации конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначен для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные.

Несанкционированный доступ – или несанкционированное воздействие – доступ к информации или воздействие на информацию, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИС.

Система защиты информации — комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИС.

1 Общие положения

Техническое задание разработано в соответствии с Приказом ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

В документе устанавливаются требования к обеспечению безопасности информации в корпоративной сети передачи данных, принадлежащей АО «ФНПЦ «ПО «Старт» им. М.В. Проценко».

2 Цели и задачи создания системы

Цель СОИБ ЗОКИИ — обеспечение устойчивого функционирования «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», в проектных режимах работы в условиях реализации угроз безопасности информации.

Задачи СОИБ ЗОКИИ:

- недопущение реализации угроз информационной безопасности;
- обнаружение существующих угроз безопасности и предупреждение их воздействия на ИС корпоративной сети передачи данных;
- обнаружение влияния угроз на ИС корпоративной сети передачи данных и локализация этого влияния;
- ликвидация последствий воздействия угроз на ИС корпоративной сети передачи данных.

3 Категория значимости

Категория значимости значимого объекта КИИ «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»: III категория значимости.

4 Перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать ЗОКИИ

Значимый объект критической информационной инфраструктуры должен соответствовать требованиям Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ, Приказу ФСТЭК России от 25 декабря 2017 г. № 239 «об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», Приказу ФСТЭК России от 21 декабря 2017 г. №235 «об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5 Перечень типов объектов защиты значимого объекта

Объекты защиты:

1 Защищаемая информация.

2 Технологическая информация:

- управляющая информация;
- технологическая информация средств доступа к системам управления;
- информация о средствах защиты информации, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения в результате обработки информации.

3 Программно-технические средства обработки:

- общесистемное и специальное программное обеспечение (операционные системы и другие);
- резервные копии общесистемного программного обеспечения;

– инструментальные средства и утилиты систем управления ресурсами ИС;

– аппаратные средства обработки информации.

4 Средства защиты информации:

– средства управления и разграничения доступа пользователей;

– средства обеспечения регистрации и учета действий с информацией;

– средства, обеспечивающие целостность данных;

– средства антивирусной защиты.

5 Объекты и помещения, в которых размещены компоненты ИС:

Местонахождение технических средств автоматизированной системы: в пределах РФ (город Заречный, Пензенская область, пр. Мира 1).

6 Требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимого объекта КИИ «Корпоративной сети передачи данных» (КСПД) АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»:

– организационные и технические меры по обеспечению безопасности значимого объекта принимаются субъектом КИИ совместно с лицом, которое эксплуатирует значимый объект (при его наличии). При этом между ними, должно быть проведено разграничение функций по обеспечению безопасности значимого объекта в ходе его эксплуатации;

– меры по обеспечению безопасности значимого объекта выбираются и реализуются с учетом угроз безопасности информации применительно на аппаратном, системном, прикладном и сетевом уровнях;

– меры по обеспечению безопасности значимого объекта КИИ принимаются субъектом КИИ самостоятельно или если необходимо с

привлечением в соответствии с законодательством РФ организаций, имеющих лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации;

– принимаемые организационные и технические меры по обеспечению безопасности значимого объекта КИИ должны соотноситься с мерами по функциональной, промышленной безопасности, а так же иными мерами по обеспечению безопасности значимого объекта КИИ. При этом меры не должны оказывать отрицательного влияния на функционирование значимого объекта в проектных режимах его работы;

– при невозможности реализации отдельных мер по обеспечению безопасности значимого объекта КИИ и (или) отсутствие возможности их применения к отдельным объектам и субъектам доступа, так же вследствие их негативного влияния на функционирование значимого объекта КИИ в проектных режимах значимого объекта, необходимо разработать и внедрить компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности;

– технические меры по обеспечению безопасности в значимом объекте КИИ реализуются посредством использования программных и программно-аппаратных средств, которые применяются для обеспечения безопасности значимых объектов КИИ – средств защиты информации (так же встроенных в общесистемное, прикладное ПО).

7 Этапы работ создания системы безопасности значимого объекта

Этапы создания СОИБ ЗОКИИ:

– этап 1. Планирование. На данном этапе устанавливаются требования, необходимые к выполнению для обеспечения безопасности каждого ЗОКИИ и

создается план мероприятий. Так же определяются актуальные угрозы безопасности информации;

– этап 2. Реализация. На данном этапе осуществляется создание сил системы безопасности ЗОКИИ, внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности ЗОКИИ, разработка организационно-распорядительной документации, которая регламентирует процессы управления информационной безопасностью;

– этап 3. Мониторинг и контроль. Основой данного этапа является проведения аудита информационной безопасности. Цель аудита информационной безопасности — определение текущего состояния информационной безопасности и какие действия необходимо предпринять в дальнейшем для создания или улучшения системы защиты информации;

– этап 4. Совершенствование. В процессе совершенствования безопасности ЗОКИИ структурное подразделение по безопасности, специалисты по безопасности должны проводить анализ функционирования системы безопасности и состояния безопасности ЗОКИИ, по результатам которого создавать предложения по развитию системы безопасности и меры по модернизации безопасности ЗОКИИ.

8 Требования к применяемым программным и программно-аппаратным средствам

Требования к применяемым программным и программно-аппаратным средствам:

– программные и программно-аппаратные средства, применяемые в значимом объекте КИИ, должны эксплуатироваться в соответствии с инструкциями по эксплуатации, которые разрабатываются разработчиками этих средств, и другой эксплуатационной документацией;

– программные и программно-аппаратные средства, применяемые в значимом объекте КИИ, должны быть обеспечены гарантийной и (или) технической поддержкой.

9 Требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре)

Требования к защите средств и систем, обеспечивающих функционирование значимого объекта:

– для обеспечения безопасности значимых объектов КИИ необходимо применять средства защиты информации, которые прошли оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки;

– средства защиты информации, применяемые в значимом объекте КИИ должны эксплуатироваться в соответствии с инструкциями по эксплуатации, которые разрабатываются разработчиками этих средств, и другой эксплуатационной документацией;

– средства защиты информации, применяемые в значимом объекте КИИ должны быть обеспечены гарантийной и (или) технической поддержкой.

10 Требования к информационному взаимодействию значимого объекта с иными объектами КИИ, а также иными ИС, АСУ или ИТКС

Взаимодействие значимого объекта с иными объектами КИИ, и иными ИС, АСУ, ИТКС, должно осуществляться с помощью сертифицированного межсетевого экрана.

В случаях, если при взаимодействии линия связи выходит за пределы контролируемой зоны, необходимо организовать VPN-сеть.

11 Состав и содержание мер по обеспечению безопасности КИИ

Адаптированный базовый набор мер защиты информации по обеспечению безопасности значимого объекта КИИ «Корпоративной сети передачи данных» АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» приведен в таблице М.1.

Таблица М.1— Адаптированный базовый набор мер защиты информации

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
		3
I. Идентификация и аутентификация (ИАФ)		
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+
ИАФ.2	Идентификация и аутентификация устройств	+
ИАФ.3	Управление идентификаторами	+
ИАФ.4	Управление средствами аутентификации	+
ИАФ.7	Защита аутентификационной информации при передаче	+
II. Управление доступом (УПД)		
УПД.0	Регламентация правил и процедур управления доступом	+
УПД.1	Управление учетными записями пользователей	+
УПД.2	Реализация модели управления доступом	+
УПД.4	Разделение полномочий (ролей) пользователей	+
УПД.5	Назначение минимально необходимых прав и привилегий	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+

Продолжение таблицы М.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+
ЗНИ.1	Учет машинных носителей информации	+
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+
V. Аудит безопасности (АУД)		
АУД.0	Регламентация правил и процедур аудита безопасности	+
АУД.1	Инвентаризация информационных ресурсов	+
АУД.2	Анализ уязвимостей и их устранение	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+
АУД.4	Регистрация событий безопасности	+
АУД.6	Защита информации о событиях безопасности	+
АУД.7	Мониторинг безопасности	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+
АУД.10	Проведение внутренних аудитов	+
VI. Антивирусная защита (АВЗ)		
АУД.8	Реагирование на сбои при регистрации событий безопасности	+
АУД.10	Проведение внутренних аудитов	+

Продолжение таблицы М.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
VI. Антивирусная защита (АВЗ)		
АВЗ.0	Регламентация правил и процедур антивирусной защиты	+
АВЗ.1	Реализация антивирусной защиты	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+
VIII. Обеспечение целостности (ОЦЛ)		
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+
ОЦЛ.1	Контроль целостности программного обеспечения	+
IX. Обеспечение доступности (ОДТ)		
ОДТ.0	Регламентация правил и процедур обеспечения доступности	+
ОДТ.4	Резервное копирование информации	+
ОДТ.5	Обеспечение возможности восстановления информации	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+
X. Защита технических средств (ЗТС)		
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+
ЗТС.2	Организация контролируемой зоны	+
ЗТС.3	Управление физическим доступом	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+

Продолжение таблицы М.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ЗТС.5	Защита от внешних воздействий	+
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)		
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+
ЗИС.5	Организация демилитаризованной зоны	+
ЗИС.6	Управление сетевыми потоками	+
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+
ЗИС.19	Защита информации при ее передаче по каналам связи	+
ЗИС.20	Обеспечение доверенных канала, маршрута	+
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+
ЗИС.32	Защита беспроводных соединений	+
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+
ЗИС.35	Управление сетевыми соединениями	+
XII. Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+
ИНЦ.1	Выявление компьютерных инцидентов	+

Продолжение таблицы М.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
ИНЦ.2	Информирование о компьютерных инцидентах	+
ИНЦ.3	Анализ компьютерных инцидентов	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+
XIII. Управление конфигурацией (УКФ)		
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+
УКФ.2	Управление изменениями	+
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+
XIV. Управление обновлениями программного обеспечения (ОПО)		
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+
ОПО.3	Тестирование обновлений программного обеспечения	+
ОПО.4	Установка обновлений программного обеспечения	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+

Продолжение таблицы М.1

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости
XVI. Обеспечение действий в нештатных ситуациях (ДНС)		
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+
ДНС.1	Разработка плана действий в нештатных ситуациях	+
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+
XVII. Информирование и обучение персонала (ИПО)		
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+
ИПО.2	Обучение персонала правилам безопасной работы	+
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+

Приложение Н

(обязательное)

Приказ об организации взаимодействия с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак

АО «ФНПЦ «ПО «Старт» им. М.В. Проценко»

г. Заречный

« __ » _____ 20__г. № _____

ПРИКАЗ

об организации взаимодействия с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)

В целях исполнения требований статей 5 и 9 Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»,

ПРИКАЗЫВАЮ:

1 Утвердить Акт по определению порядка взаимодействия с центрами ГосСОПКА, представленный в приложении 1 к настоящему приказу.

2 Назначить ответственным лицом за организацию взаимодействия с центрами ГосСОПКА – ФИО, должность.

3 Приказ вступает в силу со дня его подписания.

Генеральный директор АО «ФНПЦ «ПО «Старт» им. М.В. Проценко» _____ Фамилия И.О.

Приложение 1

к приказу №____

« __ » _____ 20__ г.

АО «ФНПЦ «ПО «СТАРТ» ИМ. М.В. ПРОЦЕНКО»

№_____

СОГЛАСОВАНО	УТВЕРЖДАЮ
Должность	Должность
_____Фамилия И.О.	_____Фамилия И.О.
«___» _____ 20__ г.	«___» _____ 20__ г.

АКТ

по определению порядка взаимодействия с центрами ГосСОПКА

Заречный 2020

1 Описание взаимодействия КЦ ГосСОПКА и Субъекта

1.1 КЦ ГосСОПКА

Зона ответственности КЦ ГосСОПКА:

– силы, средства, а так же объекты критической информационной инфраструктуры АО «ФНПЦ «ПО «Старт» им. М.В. Проценко», КЦ ГосСОПКА, по отношению к которым КЦ ГосСОПКА обеспечивает обнаружение, реагирование, предупреждение и ликвидацию последствий компьютерных атак;

– информационный обмен между КЦ ГосСОПКА и национальным координационным центром по компьютерным инцидентам (НКЦКИ).

Функции КЦ ГосСОПКА:

– реализация мероприятий по обнаружению, реагированию, предупреждению и ликвидации компьютерных атак в Корпоративном сегменте ГосСОПКА;

– мониторинг и регистрация событий информационной безопасности;

– регистрация, а так же сбор и анализ сведений об инцидентах информационной безопасности на объектах критической информационной инфраструктуры;

– выполнение мероприятий по предупреждению, реагированию и ликвидации последствий инцидентов информационной безопасности и компьютерных атак на объектах критической информационной инфраструктуры;

– обнаружение, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;

– своевременное обновление средств, предназначенных для функционирования КЦ ГосСОПКА, выявление ошибок в их работе;

– поддержание в актуальном состоянии информации об объектах критической информационной инфраструктуры, включая оборудование и программное обеспечение;

– предоставление в НКЦКИ сведений об инцидентах информационной безопасности на объектах критической информационной инфраструктуры и о предпринятых мерах;

– передача в НКЦКИ сведений о степени защищенности объектов критической информационной инфраструктуры;

– оказание содействия Субъекту по реагированию и ликвидации последствий компьютерных инцидентов и атак;

– уведомление Субъекта об инцидентах информационной безопасности и компьютерных атаках, и оказание содействия по устранению причин их возникновения;

– предоставление Субъекту информации об актуальных уязвимостях, полученных от НКЦКИ.

КЦ ГосСОПКА имеет право:

– направлять уведомления и запросы Субъекту по вопросам, связанным с обнаружением, реагированием, предупреждением и ликвидацией последствий компьютерных атак;

– проводить проверку материалов, которые предоставляет Субъект;

– формировать предложения по совершенствованию нормативной правовой базы по защите информации.

1.2 Субъект

Зона ответственности Субъекта:

– силы и средства, а так же объекты критической информационной инфраструктуры, в отношении которых Субъект обеспечивает обнаружение, реагирование, предупреждение и ликвидацию последствий компьютерных атак;

– информационный обмен между КЦ ГосСОПКА, Субъектом и НКЦКИ.

Функции Субъекта:

– определение перечня объектов критической информационной инфраструктуры, необходимого для подключения к технической инфраструктуре КЦ ГосСОПКА;

– мониторинг событий информационной безопасности на объектах критической информационной инфраструктуры;

– регистрация инцидентов информационной безопасности;

– реализация сбора и анализа сведений об уязвимостях программного обеспечения и оборудования;

– проведение мероприятий по предупреждению, реагированию и ликвидации последствий компьютерных инцидентов и компьютерных атак;

– формирование информации об объектах критической информационной инфраструктуры, а так же оборудование и программное обеспечение;

– реализация полученных от КЦ ГосСОПКА рекомендаций по противодействию компьютерным атакам и устранению уязвимостей;

– осуществление информационного взаимодействия с региональными центрами НКЦКИ по вопросам предупреждения, реагирования, и ликвидации последствий инцидентов и компьютерных атак.

Субъект должен направить в КЦ ГосСОПКА:

– заявку на подключение к КЦ ГосСОПКА;

– перечень объектов критической информационной инфраструктуры, с указанием категории значимости;

– перечень используемого оборудования и программного обеспечения;

– перечень используемых средств защиты информации;

– список лиц ответственных за обнаружение, реагирование, предупреждение, и ликвидации последствий компьютерных атак.

Субъект должен предоставлять в КЦ ГосСОПКА:

– сведения об инцидентах информационной безопасности и компьютерных атаках, а так же информации о предпринятых мерах;

– сведения об актуальных уязвимостях;

– информацию о составе объектов критической информационной инфраструктуры.

Субъект имеет право:

– направлять запрос в КЦ ГосСОПКА по рекомендациям о ликвидации последствий компьютерных атак;

– формировать предложения по совершенствованию нормативной правовой базы по защите информации.

2 Представление Субъектом информации в КЦ ГосСОПКА

Способы информирования КЦ ГосСОПКА:

- по телекоммуникационным каналам связи;
- по электронной почте;
- посредством телефонной связи.

Сроки информирования.

Информация, связанная с функционированием объектов критической информационной инфраструктуры, направляется Субъектом в КЦ ГосСОПКА, не позднее 3-х часов с момента обнаружения компьютерного инцидента.

3 Обязанности Субъекта

Субъект должен производить постоянный мониторинг событий информационной безопасности.

Субъект должен осуществлять сбор и обработку событий, которые связанны с нарушением информационной безопасности, поступающих от операционных систем, средств обнаружения вторжений, межсетевых экранов, средств предотвращения утечек данных, антивирусного программного обеспечения, телекоммуникационного оборудования, прикладных сервисов и программного обеспечения, средств контроля (анализа) защищенности, средств управления телекоммуникационным оборудованием и сетями связи, систем мониторинга состояния телекоммуникационного оборудования, систем мониторинга качества обслуживания, а также иных средств и систем защиты информации и систем мониторинга, эксплуатируемых Субъектом.

Субъект должен проводить регистрацию инцидента информационной безопасности по форме:

- контактная информация сотрудника, обнаружившего инцидент;
- время возникновения инцидента;
- время обнаружения инцидента;
- перечень информационных ресурсов, которые подверглись компьютерной атаке;
- другие сведения о компьютерной атаке.

Регистрация инцидента информационной безопасности производится в бумажном или электронном виде.

При обнаружении инцидента информационной безопасности Субъект должен оповестить КЦ ГосСОПКА.