ПРАВИТЕЛЬСТВО САРАТОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 8 мая 2020 года № 370-П

г. Саратов

О внесении изменений в постановление Правительства Саратовской области от 19 февраля 2016 года № 60-П

На основании Устава (Основного Закона) Саратовской области Правительство Саратовской области ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правительства Саратовской области от 19 февраля 2016 года № 60-П «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти области, подведомственных им учреждениях и предприятиях» следующие изменения:

в приложении:

пункты 1.2, 1.3 изложить в следующей редакции:

«1.2. Актуальные угрозы безопасности содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) в органах исполнительной власти области, входящих в структуру органов исполнительной власти Саратовской области, утвержденную постановлением Губернатора Саратовской области от 8 ноября 2017 года № 393, подведомственных им учреждениях и предприятиях (далее – государственные органы). Актуальные угрозы безопасности также содержат совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак на ИСПДн, в случае применения в них средств криптографической защиты информации для обеспечения безопасности персональных данных. Настоящие Актуальные угрозы безопасности применяются на этапах создания, модернизации ИСПДн для определения и оценки угроз безопасности персональных данных, а также в ходе эксплуатации ИСПДн при периодическом пересмотре актуальности угроз безопасности персональных данных.

1.3. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в Актуальных угрозах безопасности, подлежат адаптации в ходе разработки операторами ИСПДн частных моделей угроз

безопасности информации. Адаптация Актуальных угроз безопасности направлена на уточнение перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн. В процессе этой работы проводится анализ структурно-функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий и особенностей ее функционирования и осуществляется исключение угроз безопасности, которые непосредственно связаны с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн. По результатам анализа делается вывод об отнесении ИСПДн к одному из видов ИСПДн, приведенных в пункте 1.6 настоящего документа.»;

пункт 1.6.2 изложить в следующей редакции:

«1.6.2. ИСПДн обеспечения специальной деятельности, предназначенные для автоматизации или информационной поддержки предоставления государственных услуг, исполнения государственных функций, предусмотренных нормативными правовыми актами Саратовской области в качестве полномочий конкретного государственного органа.»;

дополнить пунктами 1.7, 1.8 следующего содержания:

«1.7. Актуальные угрозы безопасности разработаны с использованием следующих документов:

Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

постановления Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 года (далее – Базовая модель угроз безопасности);

методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 года;

методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных

данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководителем 8-го Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432.

1.8. Источником данных об угрозах безопасности информации, на основе которых определяются Актуальные угрозы безопасности, являются:

банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru, далее – Банк данных угроз);

Базовая модель угроз безопасности.»;

в пункте 2.3 слова «, управления кадровым резервом, проведения аттестации, повышения квалификации и других функций, связанных с управлением персоналом государственных органов. В ИСПДн управление персоналом обрабатываются ПДн сотрудников органа исполнительной власти, граждан, подавших сведения для участия в конкурсе на замещение вакантных должностей государственной гражданской службы и о включении в кадровый резерв, а также граждан, претендующих на замещение должностей руководителей подведомственных им учреждений и предприятий: фамилия, имя, отчество; дата и место рождения; адрес места жительства; паспортные данные; сведения для заполнения личных карточек работников формы № Т-2; сведения из трудовой книжки; дополнительный перечень информации, имеющей характер персональных данных работников» исключить;

в пункте 2.4 слова «В ИСПДн управление финансами обрабатываются: фамилия, имя, отчество; дата и место рождения; паспортные данные; адрес места жительства; номер телефона, идентификационный номер налогоплательщика (далее – ИНН), страховой номер индивидуального лицевого счета (СНИЛС), табельный номер, наименование должности, номер приказа и дата приема на работу (увольнения), номер лицевого счета для перечисления денежного содержания и иных выплат работнику; фамилия, имя, отчество, паспортные данные, места жительства, наименование должности, номер телефона, ИНН, банковские платежные реквизиты граждан, являющихся стороной гражданско-правовых договоров о выполнении работ, оказании услуг.» исключить;

пункт 3.8 признать утратившим силу;

в пункте 4.7 слова «Источники атак на объекты ИСПДн располагают обобщенными возможностями в соответствии с таблицей № 2.» заменить словами «В случае, если оператором ИСПДн принято решение о применении СКЗИ для обеспечения безопасности персональных данных в ИСПДн, то при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в данной ИСПДн, оператор дополнительно формирует совокупность предположений о возможностях источников атак, которые могут использоваться при создании способов, подготовке и проведении атак на ИСПДн, в которых применяются СКЗИ. Источники атак на объекты ИСПДн располагают обобщенными возможностями в соответствии с таблицей № 2.»;

в пункте 4.8 таблицу № 3 изложить в следующей редакции:

«Таблица № 3

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использо-вания (применения) для построения и реализации атак	Обоснование отсутствия актуальных угроз безопасности
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены

			входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ, используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты
1.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ; помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения

1.3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	актуально	
1.4.	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	актуально	
2.1.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия только для санкционированного прохода

2.2.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в КЗ и помещения, где располагается средство вычислительной техники (далее – СВТ), на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;

			представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ, используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне КЗ, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
3.3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности

4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в КЗ и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ, используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты
4.2.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3.	Возможность воздействовать на любые компоненты СКЗИ и СФ	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

»;

дополнить пунктом 5.12 следующего содержания:

«5.12. В случае обработки персональных данных в государственных информационных системах регионального масштаба угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности). В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (http://bdu.fstec.ru), ведение которого осуществляется ФСТЭК России. Для государственных информационных систем регионального масштаба актуальными являются следующие дополнительные угрозы безопасности информации, указанные в таблице № 7.

Таблица № 7

Идентификатор	**Наименование угрозы безопасности информации**	**Актуальность угрозы безопасности**
УБИ.1	Угроза автоматического распространения вредоносного кода в грид-системе	не актуально
УБИ.2	Угроза агрегирования данных, передаваемых в грид-системе	не актуально
УБИ.3	Угроза анализа криптографических алгоритмов и их реализации	не актуально
УБИ.4	Угроза аппаратного сброса пароля BIOS	актуально
УБИ.5	Угроза внедрения вредоносного кода в BIOS	не актуально
УБИ.6	Угроза внедрения кода или данных	актуально
УБИ.7	Угроза воздействия на программы с высокими привилегиями	актуально
УБИ.8	Угроза восстановления аутентификационной информации	актуально
УБИ.9	Угроза восстановления предыдущей уязвимой версии BIOS	актуально
УБИ.10	Угроза выхода процесса за пределы виртуальной машины	актуально
УБИ.11	Угроза деавторизации санкционированного клиента беспроводной сети	не актуально
УБИ.12	Угроза деструктивного изменения конфигурации/среды окружения программ	актуально
УБИ.13	Угроза деструктивного использования декларированного функционала BIOS	актуально
УБИ.14	Угроза длительного удержания вычислительных ресурсов пользователями	актуально

УБИ.15	Угроза доступа к защищаемым файлам с использованием обходного пути	актуально
УБИ.16	Угроза доступа к локальным файлам сервера при помощи URL	актуально
УБИ.17	Угроза доступа/перехвата/изменения HTTP cookies	актуально
УБИ.18	Угроза загрузки нештатной операционной системы	актуально
УБИ.19	Угроза заражения DNS-кеша	актуально
УБИ.20	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	актуально
УБИ.21	Угроза злоупотребления доверием потребителей облачных услуг	актуально
УБИ.22	Угроза избыточного выделения оперативной памяти	актуально
УБИ.23	Угроза изменения компонентов системы	актуально
УБИ.24	Угроза изменения режимов работы аппаратных элементов компьютера	актуально
УБИ.25	Угроза изменения системных и глобальных переменных	актуально
УБИ.26	Угроза искажения XML-схемы	актуально
УБИ.27	Угроза искажения вводимой и выводимой на периферийные устройства информации	актуально
УБИ.28	Угроза использования альтернативных путей доступа к ресурсам	актуально
УБИ.29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	не актуально
УБИ.30	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	актуально
УБИ.31	Угроза использования механизмов авторизации для повышения привилегий	актуально
УБИ.32	Угроза использования поддельных цифровых подписей BIOS	не актуально
УБИ.33	Угроза использования слабостей кодирования входных данных	актуально
УБИ.34	Угроза использования слабостей протоколов сетевого/локального обмена данными	актуально
УБИ.35	Угроза использования слабых криптографических алгоритмов BIOS	не актуально
УБИ.36	Угроза исследования механизмов работы программы	актуально
УБИ.37	Угроза исследования приложения через отчеты об ошибках	актуально
УБИ.38	Угроза исчерпания вычислительных ресурсов хранилища больших данных	не актуально
УБИ.39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	актуально

УБИ.40	Угроза конфликта юрисдикций различных стран	не актуально
УБИ.41	Угроза межсайтового скриптинга	актуально
УБИ.42	Угроза межсайтовой подделки запроса	актуально
УБИ.43	Угроза нарушения доступности облачного сервера	актуально
УБИ.44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	актуально
УБИ.45	Угроза нарушения изоляции среды исполнения BIOS	актуально
УБИ.46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	актуально
УБИ.47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	не актуально
УБИ.48	Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	актуально
УБИ.49	Угроза нарушения целостности данных кеша	актуально
УБИ.50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	не актуально
УБИ.51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	актуально
УБИ.52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	актуально
УБИ.53	Угроза невозможности управления правами пользователей BIOS	актуально
УБИ.54	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	актуально
УБИ.55	Угроза незащищенного администрирования облачных услуг	актуально
УБИ.56	Угроза некачественного переноса инфраструктуры в облако	актуально
УБИ.57	Угроза неконтролируемого копирования данных внутри хранилища больших данных	не актуально
УБИ.58	Угроза неконтролируемого роста числа виртуальных машин	актуально
УБИ.59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	актуально
УБИ.60	Угроза неконтролируемого уничтожения информации хранилищем больших данных	не актуально
УБИ.61	Угроза некорректного задания структуры данных транзакции	актуально
УБИ.62	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	актуально

УБИ.63	Угроза некорректного использования функционала программного обеспечения	актуально
УБИ.64	Угроза некорректной реализации политики лицензирования в облаке	актуально
УБИ.65	Угроза неопределенности в распределении ответственности между ролями в облаке	актуально
УБИ.66	Угроза неопределенности ответственности за обеспечение безопасности облака	актуально
УБИ.67	Угроза неправомерного ознакомления с защищаемой информацией	актуально
УБИ.68	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	актуально
УБИ.69	Угроза неправомерных действий в каналах связи	актуально
УБИ.70	Угроза непрерывной модернизации облачной инфраструктуры	актуально
УБИ.71	Угроза несанкционированного восстановления удалённой защищаемой информации	актуально
УБИ.72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	актуально
УБИ.73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	актуально
УБИ.74	Угроза несанкционированного доступа к аутентификационной информации	актуально
УБИ.75	Угроза несанкционированного доступа к виртуальным каналам передачи	актуально
УБИ.76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	актуально
УБИ.77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	актуально
УБИ.78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	актуально
УБИ.79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	актуально
УБИ.80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	актуально
УБИ.81	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	не актуально

УБИ.82	Угроза несанкционированного доступа к сегментам вычислительного поля	не актуально
УБИ.83	Угроза несанкционированного доступа к системе по беспроводным каналам	не актуально
УБИ.84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	актуально
УБИ.85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	актуально
УБИ.86	Угроза несанкционированного изменения аутентификационной информации	актуально
УБИ.87	Угроза несанкционированного использования привилегированных функций BIOS	актуально
УБИ.88	Угроза несанкционированного копирования защищаемой информации	актуально
УБИ.89	Угроза несанкционированного редактирования реестра	актуально
УБИ.90	Угроза несанкционированного создания учетной записи пользователя	актуально
УБИ.91	Угроза несанкционированного удаления защищаемой информации	актуально
УБИ.92	Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам	не актуально
УБИ.93	Угроза несанкционированного управления буфером	актуально
УБИ.94	Угроза несанкционированного управления синхронизацией и состоянием	не актуально
УБИ.95	Угроза несанкционированного управления указателями	актуально
УБИ.96	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	не актуально
УБИ.97	Угроза несогласованности правил доступа к большим данным	не актуально
УБИ.98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	актуально
УБИ.99	Угроза обнаружения хостов	актуально
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	актуально
УБИ.101	Угроза общедоступности облачной инфраструктуры	актуально
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	актуально
УБИ.103	Угроза определения типов объектов защиты	актуально
УБИ.104	Угроза определения топологии вычислительной сети	актуально

УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	не актуально
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	не актуально
УБИ.107	Угроза отключения контрольных датчиков	не актуально
УБИ.108	Угроза ошибки обновления гипервизора	актуально
УБИ.109	Угроза перебора всех настроек и параметров приложения	актуально
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	не актуально
УБИ.111	Угроза передачи данных по скрытым каналам	актуально
УБИ.112	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	не актуально
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	актуально
УБИ.114	Угроза переполнения целочисленных переменных	актуально
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	актуально
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	актуально
УБИ.117	Угроза перехвата привилегированного потока	актуально
УБИ.118	Угроза перехвата привилегированного процесса	актуально
УБИ.119	Угроза перехвата управления гипервизором	актуально
УБИ.120	Угроза перехвата управления средой виртуализации	актуально
УБИ.121	Угроза повреждения системного реестра	актуально
УБИ.122	Угроза повышения привилегий	актуально
УБИ.123	Угроза подбора пароля BIOS	актуально
УБИ.124	Угроза подделки записей журнала регистрации событий	актуально
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	не актуально
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	не актуально
УБИ.127	Угроза подмены действия пользователя путем обмана	актуально
УБИ.128	Угроза подмены доверенного пользователя	актуально
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	актуально
УБИ.130	Угроза подмены содержимого сетевых ресурсов	актуально
УБИ.131	Угроза подмены субъекта сетевого доступа	актуально
УБИ.132	Угроза получения предварительной информации об объекте защиты	актуально
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	не актуально

УБИ.134	Угроза потери доверия к поставщику облачных услуг	актуально
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	актуально
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	не актуально
УБИ.137	Угроза потери управления облачными ресурсами	актуально
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе ее в облако	актуально
УБИ.139	Угроза преодоления физической защиты	актуально
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	актуально
УБИ.141	Угроза привязки к поставщику облачных услуг	актуально
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	актуально
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	актуально
УБИ.144	Угроза программного сброса пароля BIOS	актуально
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	актуально
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	не актуально
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	не актуально
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	не актуально
УБИ.149	Угроза сбоя обработки специальным образом измененных файлов	актуально
УБИ.150	Угроза сбоя процесса обновления BIOS	актуально
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	не актуально
УБИ.152	Угроза удаления аутентификационной информации	актуально
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	актуально
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	актуально
УБИ.155	Угроза утраты вычислительных ресурсов	актуально
УБИ.156	Угроза утраты носителей информации	актуально
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	актуально

УБИ.158	Угроза форматирования носителей информации	актуально
УБИ.159	Угроза «форсированного веб-браузинга»	актуально
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	актуально
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	не актуально
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	не актуально
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	актуально
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	актуально
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	актуально
УБИ.166	Угроза внедрения системной избыточности	актуально
УБИ.167	Угроза заражения компьютера при посещении неблагонадежных сайтов	актуально
УБИ.168	Угроза «кражи» учетной записи доступа к сетевым сервисам	актуально
УБИ.169	Угроза наличия механизмов разработчика	актуально
УБИ.170	Угроза неправомерного шифрования информации	актуально
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	актуально
УБИ.172	Угроза распространения «почтовых червей»	актуально
УБИ.173	Угроза «спама» веб-сервера	актуально
УБИ.174	Угроза «фарминга»	актуально
УБИ.175	Угроза «фишинга»	актуально
УБИ.176	Угроза нарушения технологического/ производственного процесса из-за временны́х задержек, вносимых средством защиты	актуально
УБИ.177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	актуально
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	актуально
УБИ.179	Угроза несанкционированной модификации защищаемой информации	актуально
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	актуально
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	не актуально
УБИ.182	Угроза физического устаревания аппаратных компонентов	актуально

УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	не актуально
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	не актуально
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	актуально
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	актуально
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	актуально
УБИ.188	Угроза подмены программного обеспечения	актуально
УБИ.189	Угроза маскирования действий вредоносного кода	актуально
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	актуально
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	актуально
УБИ.192	Угроза использования уязвимых версий программного обеспечения	актуально
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	актуально
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	не актуально
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	не актуально
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	не актуально
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	актуально
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	актуально
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	не актуально
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	не актуально
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	актуально
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	не актуально
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	не актуально

УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	не актуально
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	актуально
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	не актуально
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	не актуально
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	актуально
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	актуально
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	не актуально
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечениям администрирования информационных систем	актуально
УБИ.212	Угроза перехвата управления информационной системой	актуально
УБИ.213	Угроза обхода многофакторной аутентификации	не актуально
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	актуально
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	актуально
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	не актуально
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	актуально

».

2. Министерству информации и печати области опубликовать настоящее постановление в течение десяти дней со дня его подписания.

3. Настоящее постановление вступает в силу со дня его подписания.

Вице-губернатор Саратовской области –
Председатель Правительства
Саратовской области **А.М. Стрелюхин**

ПРАВИТЕЛЬСТВО САРАТОВСКОЙ ОБЛАСТИ * УПРАВЛЕНИЕ ДЕЛОПРОИЗВОДСТВА И КОНТРОЛЯ