BIOS:

004 Угроза аппаратного сброса пароля BIOS,

005 Угроза внедрения вредоносного кода в BIOS,

009 Угроза восстановления предыдущей уязвимой версии BIOS,

013 Угроза деструктивного использования декларированного функционала BIOS,

032 Угроза использования поддельных цифровых подписей BIOS,

035 Угроза использования слабых криптографических алгоритмов BIOS,

039 Угроза исчерпания запаса ключей, необходимых для обновления BIOS,

045 Угроза нарушения изоляции среды исполнения BIOS,

053 Угроза невозможности управления правами пользователей BIOS,

072 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS,

087 Угроза несанкционированного использования привилегированных функций BIOS,

123 Угроза подбора пароля BIOS,

129 Угроза подмены резервной копии программного обеспечения BIOS,

144 Угроза программного сброса пароля BIOS,

150 Угроза сбоя процесса обновления BIOS,

154 Угроза установки уязвимых версий обновления программного обеспечения BIOS

Грид-системы/РИС:

001 Угроза автоматического распространения вредоносного кода в грид-системе,

002 Угроза агрегирования данных, передаваемых в грид-системе,

047 Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке,

081 Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы,

084 Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети

085 Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации,

110 Угроза перегрузки грид-системы вычислительными заданиями,

147 Угроза распространения несанкционированно повышенных прав на всю грид-систему

Машинное обучение:

218 Угроза раскрытия информации о модели машинного обучения,

219 Угроза хищения обучающих данных,

220 Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта,

221 Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных,

222 Угроза подмены модели машинного обучения

Мобильные устройства:

184 Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства,

194 Угроза несанкционированного использования привилегированных функций мобильного устройства,

196 Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве,

199 Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов,

200 Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов,

202 Угроза несанкционированной установки приложений на мобильные устройства

Виртуальные машины и гипервизор:

010 Угроза выхода процесса за пределы виртуальной машины,

044 Угроза нарушения изоляции пользовательских данных внутри виртуальной машины,

048 Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин,

052 Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения,

058 Угроза неконтролируемого роста числа виртуальных машин,

073 Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети,

076 Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети,

078 Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети,

079 Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин,

108 Угроза ошибки обновления гипервизора,

119 Угроза перехвата управления гипервизором,

120 Угроза перехвата управления средой виртуализации

Облако:

020 Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг,

021 Угроза злоупотребления доверием потребителей облачных услуг,

043 Угроза нарушения доступности облачного сервера,

054 Угроза недобросовестного исполнения обязательств поставщиками облачных услуг,

055 Угроза незащищённого администрирования облачных услуг,

056 Угроза некачественного переноса инфраструктуры в облако,

064 Угроза некорректной реализации политики лицензирования в облаке,

065 Угроза неопределённости в распределении ответственности между ролями в облаке,

066 Угроза неопределённости ответственности за обеспечение безопасности облака,

070 Угроза непрерывной модернизации облачной инфраструктуры,

071 Угроза несанкционированного восстановления удалённой защищаемой информации,

076 Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети,

077 Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение,

096 Угроза несогласованности политик безопасности элементов облачной инфраструктуры,

101 Угроза общедоступности облачной инфраструктуры,

134 Угроза потери доверия к поставщику облачных услуг,

135 Угроза потери и утечки данных, обрабатываемых в облаке,

137 Угроза потери управления облачными ресурсами,

138 Угроза потери управления собственной инфраструктурой при переносе её в облако,

141 Угроза привязки к поставщику облачных услуг,

142 Угроза приостановки оказания облачных услуг вследствие технических сбоев,

164 Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре,

Сети:

011 Угроза деавторизации санкционированного клиента беспроводной сети,

019 Угроза заражения DNS-кеша,

033 Угроза использования слабостей кодирования входных данных,

034 Угроза использования слабостей протоколов сетевого/локального обмена данными,

069 Угроза неправомерных действий в каналах связи,

075 Угроза несанкционированного доступа к виртуальным каналам передачи,

080 Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети,

083 Угроза несанкционированного доступа к системе по беспроводным каналам,

098 Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб,

099 Угроза обнаружения хостов,

103 Угроза определения типов объектов защиты,

104 Угроза определения топологии вычислительной сети,

111 Угроза передачи данных по скрытым каналам,

116 Угроза перехвата данных, передаваемых по вычислительной сети,

125 Угроза подключения к беспроводной сети в обход процедуры аутентификации,

126 Угроза подмены беспроводного клиента или точки доступа,

128 Угроза подмены доверенного пользователя,

130 Угроза подмены содержимого сетевых ресурсов,

131 Угроза подмены субъекта сетевого доступа,

133 Угроза получения сведений о владельце беспроводного устройства

153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов,

168 Угроза «кражи» учётной записи доступа к сетевым сервисам,

170 Угроза неправомерного шифрования информации,

171 Угроза скрытного включения вычислительного устройства в состав бот-сети,

193 Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика,

212 Угроза перехвата управления информационной системой

Суперкомпьютеры и большие данные:

029 Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами,

038 Угроза исчерпания вычислительных ресурсов хранилища больших данных

050 Угроза неверного определения формата входных данных, поступающих в хранилище больших данных

057 Угроза неконтролируемого копирования данных внутри хранилища больших данных

059 Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов

060 Угроза неконтролируемого уничтожения информации хранилищем больших данных

082 Угроза несанкционированного доступа к сегментам вычислительного поля

097 Угроза несогласованности правил доступа к большим данным

102 Угроза опосредованного управления группой программ через совместно используемые данные

105 Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных

106 Угроза отказа в обслуживании системой хранения данных суперкомпьютера

136 Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных

146 Угроза прямого обращения к памяти вычислительного поля суперкомпьютера

148 Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных

161 Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями

ОС и ПО:

003 Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации,

006 Угроза внедрения кода или данных,

007 Угроза воздействия на программы с высокими привилегиями,

012 Угроза деструктивного изменения конфигурации/среды окружения программ,

014 Угроза длительного удержания вычислительных ресурсов пользователями,

015 Угроза доступа к защищаемым файлам с использованием обходного пути,

018 Угроза загрузки нештатной операционной системы,

022 Угроза избыточного выделения оперативной памяти,

023 Угроза изменения компонентов информационной (автоматизированной) системы,

025 Угроза изменения системных и глобальных переменных,

031 Угроза использования механизмов авторизации для повышения привилегий,

036 Угроза исследования механизмов работы программы,

037 Угроза исследования приложения через отчёты об ошибках,

046 Угроза неправомерного ознакомления с защищаемой информацией,

049 Угроза нарушения целостности данных кеша,

051 Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания

061 Угроза некорректного задания структуры данных транзакции

063 Угроза некорректного использования функционала программного и аппаратного обеспечения

068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением

088 Угроза несанкционированного копирования защищаемой информации

089 Угроза несанкционированного редактирования реестра

090 Угроза несанкционированного создания учётной записи пользователя

091 Угроза несанкционированного удаления защищаемой информации

093 Угроза несанкционированного управления буфером

094 Угроза несанкционированного управления синхронизацией и состоянием

095 Угроза несанкционированного управления указателями

109 Угроза перебора всех настроек и параметров приложения

114 Угроза переполнения целочисленных переменных

117 Угроза перехвата привилегированного потока

118 Угроза перехвата привилегированного процесса

121 Угроза повреждения системного реестра

122 Угроза повышения привилегий

124 Угроза подделки записей журнала регистрации событий

132 Угроза получения предварительной информации об объекте защиты

140 Угроза приведения системы в состояние «отказ в обслуживании»

145 Угроза пропуска проверки целостности программного обеспечения

149 Угроза сбоя обработки специальным образом изменённых файлов

155 Угроза утраты вычислительных ресурсов

162 Угроза эксплуатации цифровой подписи программного кода

163 Угроза перехвата исключения/сигнала из привилегированного блока функций

165 Угроза включения в проект не достоверно испытанных компонентов

166 Угроза внедрения системной избыточности

169 Угроза наличия механизмов разработчика

176 Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты

177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью

178 Угроза несанкционированного использования системных и сетевых утилит

179 Угроза несанкционированной модификации защищаемой информации

185 Угроза несанкционированного изменения параметров настройки средств защиты информации

187 Угроза несанкционированного воздействия на средство защиты информации

188 Угроза подмены программного обеспечения

189 Угроза маскирования действий вредоносного кода

191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

192 Угроза использования уязвимых версий программного обеспечения

195 Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы

198 Угроза скрытной регистрации вредоносной программой учетных записей администраторов

205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты

206 Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем

208 Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники

209 Угроза несанкционированного доступа к защищаемой памяти ядра процессора

210 Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения

211 Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем

214 Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации

215 Угроза несанкционированного доступа к системе при помощи сторонних сервисов,

217 Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

WEB и браузеры:

016 Угроза доступа к локальным файлам сервера при помощи URL,

017 Угроза доступа/перехвата/изменения HTTP cookies,

026 Угроза искажения XML-схемы,

028 Угроза использования альтернативных путей доступа к ресурсам,

041 Угроза межсайтового скриптинга,

042 Угроза межсайтовой подделки запроса

062 Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера

151 Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL

159 Угроза «форсированного веб-браузинга»

167 Угроза заражения компьютера при посещении неблагонадёжных сайтов

172 Угроза распространения «почтовых червей»

173 Угроза «спама» веб-сервера

174 Угроза «фарминга»

175 Угроза «фишинга»

186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент

190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет

197 Угроза хищения аутентификационной информации из временных файлов cookie

201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере

Аутентификация:

008 Угроза восстановления и/или повторного использования аутентификационной информации,

030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию

046 Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия

074 Угроза несанкционированного доступа к аутентификационной информации

086 Угроза несанкционированного изменения аутентификационной информации

100 Угроза обхода некорректно настроенных механизмов аутентификации

152 Угроза удаления аутентификационной информации

181 Угроза перехвата одноразовых паролей в режиме реального времени

213 Угроза обхода многофакторной аутентификации

Аппаратура:

024 Угроза изменения режимов работы аппаратных элементов компьютера

027 Угроза искажения вводимой и выводимой на периферийные устройства информации

092 Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам

107 Угроза отключения контрольных датчиков

112 Угроза передачи запрещённых команд на оборудование с числовым программным управлением

113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники

115 Угроза перехвата вводимой и выводимой на периферийные устройства информации

139 Угроза преодоления физической защиты

143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

156 Угроза утраты носителей информации

157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

158 Угроза форматирования носителей информации

160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации

180 Угроза отказа подсистемы обеспечения температурного режима

182 Угроза физического устаревания аппаратных компонентов

183 Угроза перехвата управления автоматизированной системой управления технологическими процессами

203 Угроза утечки информации с неподключенных к сети Интернет компьютеров

204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров

207 Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)

216 Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах

Право:

40 Угроза конфликта юрисдикций различных стран