УПРАВЛЕНИЕ ДЕЛАМИ
ГУБЕРНАТОРА АСТРАХАНСКОЙ ОБЛАСТИ
(АГЕНТСТВО АСТРАХАНСКОЙ ОБЛАСТИ)

П О С Т А Н О В Л Е Н И Е

«23» 07 2019 г. № 4-П

г. Астрахань

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в управлении делами Губернатора Астраханской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» управление делами Губернатора Астраханской области (агентство Астраханской области)
ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в управлении делами Губернатора Астраханской области согласно приложению к настоящему постановлению.

2. Отделу нормативно-правового и кадрового обеспечения:

- в семидневный срок после дня первого официального опубликования направить копию настоящего постановления, а также сведения об источниках его официального опубликования в Управление Министерства юстиции Российской Федерации по Астраханской области;

- не позднее семи рабочих дней со дня подписания направить копию настоящего постановления в прокуратуру Астраханской области.

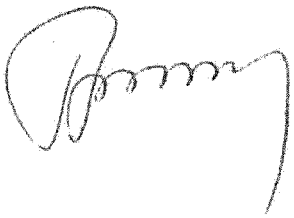
3. Отделу организационно-документационного обеспечения и контроля разместить текст настоящего постановления на официальном сайте управления делами Губернатора Астраханской области (агентства Астраханской области) в информационно-телекоммуникационной сети Интернет http://ud.astrobl.ru и направить копию постановления:

- не позднее трех рабочих дней в агентство связи и массовых коммуникаций Астраханской области для его официального опубликования;

- в семидневный срок поставщикам справочно-правовых систем «КонсультантПлюс» ООО «Астраханский информационный центр «КонсультантПлюс» и «Гарант» ООО «Астрахань-Гарант-Сервис».

000345

4. Настоящее постановление вступает в силу со дня его официального опубликования.

И. о. управляющего делами  А.Я. Жабин

Приложение к постановлению управления делами Губернатора Астраханской области
от «23» 07 2019 № 4-11

Перечень актуальных угроз безопасности персональных данных в информационных системах персональных данных, установленных в управлении делами Губернатора Астраханской области

Угроза безопасности ПДн	Актуальность угрозы
Угрозы утечки видовой информации	Актуальная
Угрозы утечки информации по каналам ПЭМИН	Актуальная
Кража ПЭВМ	Актуальная
Кража носителей информации	Актуальная
Кража ключей и атрибутов доступа	Актуальная
Кража информации	Актуальная
Действия вредоносных программ (вирусов)	Актуальная
Недекларированные возможности программного обеспечения СЗИ	Актуальная
Установка ПО, несвязанного с исполнением служебных обязанностей	Актуальная
Утрата ключей и атрибутов доступа	Актуальная
Непреднамеренное отключение СЗИ	Актуальная
Выход из строя аппаратно-программных средств	Актуальная
Сбой системы электроснабжения	Актуальная
Стихийное бедствие	Актуальная
Кража и разглашение информации лицами, допущенными к ее обработке	Актуальная
Несанкционированное отключение СЗИ	Актуальная
Угрозы несанкционированного доступа по каналам связи	Актуальная
Угроза аппаратного сброса пароля BIOS (УБИ. 004)	Актуальная
Угроза внедрения вредоносного кода в BIOS (УБИ. 005)	Актуальная
Угроза внедрения кода или данных (УБИ. 006)	Актуальная
Угроза воздействия на программы с высокими привилегиями (УБИ. 007)	Актуальная
Угроза восстановления аутентификационной информации (УБИ. 008)	Актуальная
Угроза восстановления предыдущей уязвимой версии BIOS (УБИ. 009)	Актуальная
Угроза выхода процесса за пределы виртуальной машины (УБИ. 010)	Актуальная
Угроза деструктивного изменения конфигурации/среды окружения программ (УБИ. 012)	Актуальная

Угроза безопасности ПДн	Актуальность угрозы
Угроза деструктивного использования декларированного функционала BIOS (УБИ. 013)	Актуальная
Угроза длительного удержания вычислительных ресурсов пользователями (УБИ. 014)	Актуальная
Угроза доступа к защищаемым файлам с использованием обходного пути (УБИ. 015)	Актуальная
Угроза загрузки нештатной операционной системы (УБИ. 018)	Актуальная
Угроза заражения DNS-кеша (УБИ. 019)	Актуальная
Угроза избыточного выделения оперативной памяти (УБИ. 022)	Актуальная
Угроза изменения компонентов системы (УБИ. 023)	Актуальная
Угроза изменения режимов работы аппаратных элементов компьютера (УБИ. 024)	Актуальная
Угроза изменения системных и глобальных переменных (УБИ. 025)	Актуальная
Угроза искажения XML-схемы (УБИ. 026)	Актуальная
Угроза искажения вводимой и выводимой на периферийные устройства информации (УБИ. 027)	Актуальная
Угроза использования альтернативных путей доступа к ресурсам (УБИ. 028)	Актуальная
Угроза использования информации идентификации/аутентификации, заданной по умолчанию (УБИ. 030)	Актуальная
Угроза использования механизмов авторизации для повышения привилегий (УБИ. 031)	Актуальная
Угроза использования слабостей протоколов сетевого/локального обмена данными (УБИ. 034)	Актуальная
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины (УБИ. 044)	Актуальная
Угроза неправомерного ознакомления с защищаемой информацией (УБИ. 067)	Актуальная
Угроза неправомерных действий в каналах связи (УБИ. 069)	Актуальная
Угроза несанкционированного восстановления удалённой защищаемой информации (УБИ. 071)	Актуальная
Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети (УБИ. 073)	Актуальная
Угроза несанкционированного доступа к аутентификационной информации (УБИ. 074)	Актуальная
Угроза несанкционированного доступа к гипервизору из	Актуальная

Угроза безопасности ПДн	Актуальность угрозы
виртуальной машины и (или) физической сети (УБИ. 076)	
Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети (УБИ. 078)	Актуальная
Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети (УБИ. 080)	Актуальная
Угроза несанкционированного изменения аутентификационной информации (УБИ. 086)	Актуальная
Угроза несанкционированного копирования защищаемой информации (УБИ. 088)	Актуальная
Угроза несанкционированного редактирования реестра (УБИ. 089)	Актуальная
Угроза несанкционированного создания учётной записи пользователя (УБИ. 090)	Актуальная
Угроза несанкционированного удаления защищаемой информации (УБИ. 091)	Актуальная
Угроза несанкционированного управления буфером (УБИ. 093)	Актуальная
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб (УБИ. 098)	Актуальная
Угроза обнаружения хостов (УБИ. 099)	Актуальная
Угроза обхода некорректно настроенных механизмов аутентификации (УБИ. 100)	Актуальная
Угроза определения топологии вычислительной сети (УБИ. 104)	Актуальная
Угроза перебора всех настроек и параметров приложения (УБИ. 109)	Актуальная
Угроза передачи данных по скрытым каналам (УБИ. 111)	Актуальная
Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники (УБИ. 113)	Актуальная
Угроза перехвата вводимой и выводимой на периферийные устройства информации (УБИ. 115)	Актуальная
Угроза перехвата данных, передаваемых по вычислительной сети (УБИ. 116)	Актуальная
Угроза перехвата привилегированного потока (УБИ. 117)	Актуальная
Угроза перехвата привилегированного процесса (УБИ. 118)	Актуальная
Угроза перехвата управления гипервизором (УБИ. 119)	Актуальная
Угроза перехвата управления средой виртуализации (УБИ. 120)	Актуальная
Угроза повреждения системного реестра (УБИ. 121)	Актуальная

Угроза безопасности ПДн	Актуальность угрозы
Угроза повышения привилегий (УБИ. 122)	Актуальная
Угроза подбора пароля BIOS (УБИ. 123)	Актуальная
Угроза подделки записей журнала регистрации событий (УБИ. 124)	Актуальная
Угроза подмены действия пользователя путём обмана (УБИ. 127)	Актуальная
Угроза подмены доверенного пользователя (УБИ. 128)	Актуальная
Угроза подмены резервной копии программного обеспечения BIOS (УБИ. 129)	Актуальная
Угроза подмены содержимого сетевых ресурсов (УБИ. 130)	Актуальная
Угроза подмены субъекта сетевого доступа (УБИ. 131)	Актуальная
Угроза получения предварительной информации об объекте защиты (УБИ. 132)	Актуальная
Угроза преодоления физической защиты (УБИ. 139)	Актуальная
Угроза приведения системы в состояние «отказ в обслуживании» (УБИ. 140)	Актуальная
Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 143)	Актуальная
Угроза программного сброса пароля BIOS (УБИ. 144)	Актуальная
Угроза пропуска проверки целостности программного обеспечения (УБИ. 145)	Актуальная
Угроза сбоя процесса обновления BIOS (УБИ. 150)	Актуальная
Угроза удаления аутентификационной информации (УБИ. 152)	Актуальная
Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов (УБИ. 153)	Актуальная
Угроза установки уязвимых версий обновления программного обеспечения BIOS (УБИ. 154)	Актуальная
Угроза утраты вычислительных ресурсов (УБИ. 155)	Актуальная
Угроза утраты носителей информации (УБИ. 156)	Актуальная
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 157)	Актуальная
Угроза форматирования носителей информации (УБИ. 158)	Актуальная
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 160)	Актуальная
Угроза включения в проект не достоверно испытанных компонентов (УБИ. 165)	Актуальная
Угроза внедрения системной избыточности (УБИ. 166)	Актуальная

Угроза безопасности ПДн	Актуальность угрозы
Угроза заражения компьютера при посещении неблагонадёжных сайтов (УБИ. 167)	Актуальная
Угроза «кражи» учётной записи доступа к сетевым сервисам (УБИ. 168)	Актуальная
Угроза наличия механизмов разработчика (УБИ. 169)	Актуальная
Угроза неправомерного шифрования информации (УБИ. 170)	Актуальная
Угроза скрытного включения вычислительного устройства в состав бот-сети (УБИ. 171)	Актуальная
Угроза распространения «почтовых червей» (УБИ. 172)	Актуальная
Угроза «фарминга» (УБИ. 174)	Актуальная
Угроза «фишинга» (УБИ. 175)	Актуальная
Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты (УБИ. 176)	Актуальная
Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью (УБИ. 177)	Актуальная
Угроза несанкционированного использования системных и сетевых утилит (УБИ. 178)	Актуальная
Угроза несанкционированной модификации защищаемой информации (УБИ. 179)	Актуальная
Угроза отказа подсистемы обеспечения температурного режима (УБИ. 180)	Актуальная
Угроза несанкционированного изменения параметров настройки средств защиты информации (УБИ. 185)	Актуальная
Угроза несанкционированного воздействия на средство защиты информации (УБИ. 187)	Актуальная
Угроза подмены программного обеспечения (УБИ. 188)	Актуальная
Угроза маскирования действий вредоносного кода (УБИ. 189)	Актуальная
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет (УБИ. 190)	Актуальная
Угроза внедрения вредоносного кода в дистрибутив программного обеспечения (УБИ. 191)	Актуальная
Угроза использования уязвимых версий программного обеспечения (УБИ. 192)	Актуальная
Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика (УБИ. 193)	Актуальная
Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы (УБИ. 195)	Актуальная
Угроза хищения аутентификационной информации из	Актуальная

Угроза безопасности ПДн	Актуальность угрозы
временных файлов cookie (УБИ. 197)	
Угроза скрытной регистрации вредоносной программной учетных записей администраторов (УБИ. 198)	Актуальная
Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере (УБИ. 201)	Актуальная
Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты (УБИ.205)	Актуальная
Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники (УБИ.208)	Актуальная

Перечень возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак

№	Актуальные возможности
1	Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ
2	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ
3	Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств
4	Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используется СКЗИ
5	Применение находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ; специально разработанных АС и ПО
6	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
7	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ
8	Возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий