АДМИНИСТРАЦИЯ ПРИМОРСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

26 августа 2019 года г. Владивосток № 553-па

О перечне угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Приморского края, аппарате Администрации Приморского края, аппарате Губернатора Приморского края, органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях

На основании Устава Приморского края, в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, Администрация Приморского края

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Приморского края, аппарате Администрации Приморского края, аппарате Губернатора Приморского края, органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях.

2. Рекомендовать органам местного самоуправления муниципальных образований Приморского края при утверждении перечней угроз безопасности

персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться банком данных угроз безопасности информации, ведение которого осуществляется Федеральной службой по техническому и экспортному контролю в соответствии с Указом Президента Российской Федерации от 16 августа 2004 года № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

3. Департаменту информационной политики Приморского края обеспечить официальное опубликование настоящего постановления.

4. Контроль за исполнением настоящего постановления возложить на врио вице-губернатора Приморского края Мельникова О.А.

Губернатор края –
Глава Администрации
Приморского края О.Н. Кожемяко

УТВЕРЖДЕН

постановлением Администрации
Приморского края
от 26 августа 2019 года № 553-па

ПЕРЕЧЕНЬ
угроз безопасности персональных данных,
актуальных при обработке персональных данных
в информационных системах персональных данных,
эксплуатируемых в Администрации Приморского края, аппарате
Администрации Приморского края, аппарате Губернатора
Приморского края, органах исполнительной власти
Приморского края и подведомственных им
краевых государственных учреждениях

I. Основные угрозы безопасности персональных данных	
№ п/п	Наименование угрозы
1	2
1.1.	Угроза деструктивного использования декларированного функционала BIOS
1.2.	Угроза загрузки нештатной операционной системы
1.3.	Угроза изменения режимов работы аппаратных элементов компьютера
1.4.	Угроза неправомерного ознакомления с защищаемой информацией
1.5.	Угроза неправомерных действий в каналах связи
1.6.	Угроза несанкционированного копирования защищаемой информации
1.7.	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
1.8.	Угроза несанкционированного использования привилегированных функций BIOS
1.9.	Угроза несанкционированного удаления защищаемой информации
1.10.	Угроза повреждения системного реестра
1.11.	Угроза подмены действия пользователя путём обмана
1.12.	Угроза подмены субъекта сетевого доступа

1	2
1.13.	Угроза приведения системы в состояние «отказ в обслуживании»
1.14.	Угроза заражения компьютера при посещении неблагонадёжных сайтов
1.15.	Угроза неправомерного шифрования информации
1.16.	Угроза распространения «почтовых червей»
1.17.	Угроза «фишинга»
1.18.	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты
1.19.	Угроза отказа подсистемы обеспечения температурного режима
1.20.	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
1.21.	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
1.22.	Угроза некорректного использования функционала программного обеспечения
1.23.	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
1.24.	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
1.25.	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
1.26.	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
1.27.	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
1.28.	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
1.29.	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
1.30.	Угроза несанкционированного доступа к виртуальным каналам передачи

1	2
1.31.	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
II. Актуальные возможности источников атак, направленных на нарушение безопасности информации, защищаемой с помощью СКЗИ	
№ п/п	Описание возможности источников атак (соответствующие актуальные угрозы)
2.1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны
2.2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и СФК
2.3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и СФК
III. Возможные действия нарушителей, направленные на нарушение безопасности информации	
№ п/п	Возможные действия нарушителей (соответствующие актуальные угрозы)
3.1.	Проведение атаки при нахождении в пределах контролируемой зоны
3.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФК; - 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 СФК
3.3.	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 СФК

1	2
3.4.	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий
3.5.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФК
3.6.	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