АДМИНИСТРАЦИЯ
ЗАВИТИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

П О С Т А Н О В Л Е Н И Е

от 24.02.2026 № 227

г. Завитинск

Об утверждении Перечня недопустимых событий от реализации угроз информационной безопасности, обрабатываемой в информационных ресурсах и электронных сервисах администрации Завитинского муниципального округа, а также негативных последствий, которые могут быть результатом реализации угроз информационной безопасности

В соответствии с Указом Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

п о с т а н о в л я ю:

1. Утвердить прилагаемый Перечень недопустимых событий от реализации угроз информационной безопасности, обрабатываемой в информационных ресурсах и электронных сервисах администрации Завитинского муниципального округа, а также негативных последствий, которые могут быть результатом реализации угроз информационной безопасности.

2. Настоящее постановление подлежит официальному опубликованию в сетевом издании «Официальный портал правовой информации Завитинского муниципального округа» и размещению на официальном сайте администрации муниципального округа в информационно-телекоммуникационной сети «Интернет» http://zavadm.amurobl.ru.

3. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Завитинского
муниципального округа С.С.Линевич

УТВЕРЖДЕН
постановлением администрации
Завитинского
муниципального округа
от 24.02.2026 № 227

Перечень недопустимых событий от реализации угроз информационной безопасности, обрабатываемой в информационных ресурсах и электронных сервисах администрации Завитинского муниципального округа, а также негативных последствий, которые могут быть результатом реализации угроз информационной безопасности

№ п/п	Наименование недопустимых событий	Пороговое значение	Возможные причины и сценарии реализации недопустимых событий	Возможные негативные последствия
1	2	3	4	5
1.	Разглашение конфиденциальной информации и (или) информации с ограниченным доступом	-	**Несанкционированный доступ:** третьи лица получают доступ к информации, к которой они не должны иметь доступ. **Создание или распространение вредоносного программного обеспечения:** целенаправленная компьютерная атака на целостность информации или программного обеспечения. **Невыполнение требований нормативных правовых актов Российской Федерации регулирующих информационную безопасность:** несоблюдение требований Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности	Привлечение к административной ответственности за нарушение в области обработки конфиденциальной информации и (или) информации с ограниченным доступом. Привлечение к административной ответственности за нарушение в области обработки информации в государственных информационных системах. Нарушение деловой репутации, снижение престижа. Публикации (размещения) негативной информации в средствах массовой информации

№ п/п	Наименование недопустимых событий	Пороговое значение	Возможные причины и сценарии реализации недопустимых событий	Возможные негативные последствия
1	2	3	4	5
			критической информационной инфраструктуры Российской Федерации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 21.03.2012 № 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 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановления Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), обеспечивающем информационную безопасность органа (организации)». **Отсутствие процедур и политик:**	

№ п/п	Наименование недопустимых событий	Пороговое значение	Возможные причины и сценарии реализации недопустимых событий	Возможные негативные последствия
1	2	3	4	5
			отсутствие или несоблюдение внутренних регламентов и организационных распорядительных документов по обеспечению информационной безопасности. **Нарушение требований регуляторов в сфере информационной безопасности к информационным системам:** эксплуатация информационных систем, обрабатывающих конфиденциальную информацию и (или) информацию с ограниченным доступом без должного уровня защиты (не проведение аттестации по требованиям защиты информации, отсутствия защиты от несанкционированного доступа и т. д.). **Недостаточная осведомленность должностных лиц:** отсутствие регулярного направления должностных лиц на обучение по вопросам информационной безопасности в целях повышения квалификации	
2.	Выход из строя ключевого оборудования, необходимого для нормального функционирования администрации	Более 24 часов	**Отсутствие процедур и политик:** отсутствие или несоблюдение внутренних регламентов и организационных распорядительных документов по обеспечению информационной безопасности. **Аппаратные сбои:** выход из строя по каким –либо причинам компонентов ключевого оборудования (процессоры, материнские платы, жесткие диски, блоки	Привлечение должностных лиц к административной ответственности за неоказание государственных услуг. Нарушение деловой репутации, снижение престижа. Публикации (размещения) негативной информации в средствах массовой информации. Снижение эффективности

№ п/п	Наименование недопустимых событий	Пороговое значение	Возможные причины и сценарии реализации недопустимых событий	Возможные негативные последствия
1	2	3	4	5
			питания и системы охлаждения). **Электрические проблемы:** скачки напряжения, отключения электропитания или недостаточная защита от электромагнитных помех. **Перегрев:** недостаточное охлаждение серверов, маршрутизаторов и другого сетевого оборудования может привести к перегреву и повреждению компонентов ключевого оборудования. **Человеческий фактор:** Нарушение правил эксплуатации ключевого оборудования. **Программные сбои:** ошибки в операционных системах, драйверах или приложениях могут привести к неработоспособности оборудования, так как программное обеспечение напрямую влияет на функциональность аппаратных средств. **Износ ключевого оборудования:** устаревшее оборудование теряет свою надежность с течением времени и может перестать нормально функционировать	взаимодействия министерств с органами местного самоуправления области, а также с населением Амурской области. Несвоевременное и (или) неполное информирование населения о деятельности. Нарушения процесса предоставления государственных и муниципальных услуг в электронном виде
3.	Выход из строя и (или) работа с критическими сбоями оборудования информационных систем важных для функционирования	Более 24 часов	**Модификация данных:** несанкционированное изменение, удаление или искажение информации, что может привести к нарушению работы информационных систем или ущербу для владельца информации. **Атаки или вирусы:** кибератаки, вредоносное программное обеспечение или DDoS-атаки могут повредить или	Привлечение должностных лиц к административной ответственности за неоказание государственных услуг. Нарушение деловой репутации, снижение престижа. Публикации (размещения) негативной информации в средствах массовой информации.

№ п/п	Наименование недопустимых событий	Пороговое значение	Возможные причины и сценарии реализации недопустимых событий	Возможные негативные последствия
1	2	3	4	5
			перегрузить инфраструктуру. **Невыполнение требований по резервированию и восстановлению данных:** отсутствие необходимых мер для обеспечения доступа к данным в случае инцидента. **Недостаточная осведомленность должностных лиц:** отсутствие регулярного направления должностных лиц на обучение по вопросам информационной безопасности в целях повышения квалификации. **Отсутствие процедур и политик:** отсутствие или несоблюдение внутренних регламентов и организационных распорядительных документов по обеспечению информационной безопасности	Снижение эффективности взаимодействия министерств с органами местного самоуправления области, а также с населением Амурской области. Несвоевременное и (или) неполное информирование населения о деятельности. Нарушения процесса предоставления государственных и муниципальных услуг в электронном виде