АДМИНИСТРАЦИЯ
БЕРДЯНСКОГО ГОРОДСКОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

04.06.2026 г. № 287-П

Об утверждении Политики по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

В целях обеспечения защиты информации, соблюдения требований законодательства Российской Федерации в области информационной безопасности, в том числе Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также требований Приказа ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», Администрация Бердянского городского округа

ПОСТАНОВЛЯЕТ:

1. Утвердить Политику по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», согласно приложению к настоящему постановлению.
2. Отделу по работе с персоналом и муниципальной службы ознакомить работников Администрации Бердянского городского округа с настоящим постановлением.
3. Настоящее постановление вступает в силу со дня его официального опубликования (обнародования).
4. Настоящее постановление подлежит официальному опубликованию (обнародованию) в сетевом издании «За!Информ» https://za-inform.ru/ и размещению на официальном сайте Администрации Бердянского городского округа https://berdyansk.gosuslugi.ru/.
5. Контроль исполнения настоящего постановления возложить на заместителя главы Администрации Бердянского городского округа по общим вопросам.

Глава
Бердянского городского округа А.А. Ковганко

Приложение
УТВЕРЖДЕНО
постановлением Администрации
Бердянского городского округа
от 04.06.2026 г. № 287-П

Политика по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

1. Общие положения

1.1. Настоящая Политика по защите информации (далее - Политика) разработана в целях установления единой системы защиты информации, обрабатываемой в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», а также информации ограниченного доступа (не составляющей государственную тайну), персональных данных и иной защищаемой информации, в том числе информации в электронном виде и на официальных сайтах органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

Политика направлена на обеспечение управляемости процессов защиты информации и снижение рисков реализации угроз безопасности информации, приводящих к нарушению конфиденциальности, целостности и доступности информации, а также негативных последствий для деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

1.2. Политика разработана в соответствии с требованиями законодательства Российской Федерации в области защиты информации и информационной безопасности, в том числе Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», а также Приказа ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

Иные нормативные правовые акты и национальные стандарты в области защиты информации применяются в части, не противоречащей требованиям указанного приказа ФСТЭК России и с учетом особенностей деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

1.3. В части применения средств криптографической защиты информации (далее - СКЗИ) требования настоящей Политики реализуются в соответствии с нормативными правовыми актами Федеральной службы безопасности Российской Федерации.

1.4. Настоящая Политика определяет стратегию органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» по защите информации от несанкционированного доступа, уничтожения, изменения, блокирования, копирования и иных неправомерных действий, включая меры по обеспечению конфиденциальности, целостности и доступности информации.

2. Термины и определения

В настоящем документе использованы следующие термины и определения:

Атака на информационную систему - целенаправленное воздействие на информационную систему, ее компоненты или процессы обработки информации, создающее угрозу информационной безопасности.

Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, целостность и доступность.

Блокирование информации - временное прекращение операций по сбору, систематизации, накоплению, хранению, использованию или распространению информации.

Вредоносная программа - компьютерная программа, предназначенная для нарушения функционирования информационных систем, уничтожения, блокирования, модификации либо копирования информации без согласия владельца (статья 27 Федерального закона от 27 июля 2006 г. № 149-ФЗ).

Доступность информации — свойство информации быть доступной в требуемое время и в требуемом объеме авторизованным субъектам доступа.

Доступ к информации - возможность получения и использования информации субъектом доступа.

Защищаемая информация - информация, подлежащая защите в соответствии с законодательством Российской Федерации, нормативными правовыми актами или требованиями собственника информации.

Идентификация - процедура присвоения субъекту или объекту доступа уникального идентификатора.

Инцидент информационной безопасности - событие или серия событий, нарушающих или потенциально нарушающих политику информационной безопасности и создающих угрозу конфиденциальности, целостности или доступности информации (ГОСТ Р 57580.1-2017).

Защита информации - совокупность организационных, технических и иных мер, направленных на обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой в информационной системе, а также на предотвращение, выявление и нейтрализацию угроз безопасности информации.

Информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе использующих средства вычислительной техники и связи, реализующих информационные процессы (статья 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ).

Информационные процессы - процессы создания, сбора, обработки, накопления, хранения, поиска, передачи и уничтожения информации.

Категория информационной системы - классификационная характеристика информационной системы, определяемая в соответствии с приказом ФСТЭК России от 11 апреля 2025 г. № 117 на основе значимости обрабатываемой информации и последствий нарушения ее безопасности.

Компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки (статья 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ).

Конфиденциальность информации - свойство информации быть доступной только для субъектов, имеющих на то право.

Модель угроз — формализованное описание совокупности угроз информационной безопасности, характерных для конкретной информационной системы или класса информационных систем.

Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств информационной системы.

Обработка информации - действия (операции) с информацией, включая ее сбор,

систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (статья 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ).

Пользователь информационной системы - лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права субъектов доступа на выполнение операций с объектами доступа.

Средства защиты информации - технические, программные, программно-аппаратные и организационные средства, предназначенные для защиты информации.

Средства криптографической защиты информации (СКЗИ) - средства защиты информации, реализующие криптографические методы преобразования информации.

Угроза информационной безопасности - потенциальная возможность реализации воздействия, нарушающего конфиденциальность, целостность или доступность информации.

Уровень защищенности информационной системы - совокупность требований безопасности информации, предъявляемых к информационной системе в зависимости от ее категории и значимости обрабатываемой информации (приказ ФСТЭК России от 11 апреля 2025 г. №117).

Целостность информации - свойство информации сохранять свою структуру и содержание в процессе обработки, хранения и передачи.

В настоящем документе используются следующие сокращения:

ИБ - информационная безопасность;

ИС - информационная система;

СЗИ - средства защиты информации;

СКЗИ - средства криптографической защиты информации;

ФСБ России - Федеральная служба безопасности Российской Федерации;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю;

ЗОКИИ - значимый объект критической информационной инфраструктуры;

ОКИИ - объект критической информационной инфраструктуры.

3. Область действия Политики

3.1. Настоящая Политика распространяется на информационные системы органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», в которых осуществляется обработка информации ограниченного доступа (не составляющей государственную тайну), персональных данных, а также иной защищаемой информации, подлежащей защите в соответствии с законодательством Российской Федерации и внутренними нормативными документами органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

Требования настоящей Политики также применяются к ИС, сервисам и ресурсам органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», нарушение функционирования которых может повлечь существенные негативные последствия для деятельности указанных органов, интересов работников, контрагентов или выполнения установленных функций.

3.2. Применение требований настоящей Политики осуществляется с учетом положений приказа ФСТЭК России от 11 апреля 2025 г. № 117 и основывается на оценке значимости обрабатываемой в ИС информации и возможных последствий нарушения ее конфиденциальности, целостности и доступности.

Решение о применении требований настоящей Политики к конкретной ИС принимается по результатам ее категорирования и документально оформляется в установленном порядке.

3.3. Требования приказа ФСТЭК России от 11 апреля 2025 г. № 117 и настоящей Политики не применяются к научной информации и информационным ресурсам, предназначенным для открытого использования и распространения, при условии, что:

- в соответствующих ИС не осуществляется обработка персональных данных, информации ограниченного доступа или иной защищаемой информации;

- нарушение целостности или доступности таких информационных ресурсов не влечет существенных негативных последствий для деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

В случае изменения состава обрабатываемой информации либо архитектуры ИС, влекущего появление признаков, указанных в пункте 3.1 настоящей Политики, применение требований Политики подлежит обязательному пересмотру.

3.4. Настоящая Политика распространяется на информационно-телекоммуникационную инфраструктуру, технические средства обработки информации, программное обеспечение, сети и каналы передачи данных, а также автоматизированные рабочие места пользователей в той части, в которой они используются для функционирования ИС, подпадающих под действие настоящей Политики.

3.5. Соблюдение требований настоящей Политики является обязательным для:

- всех работников органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», использующих ИС и (или) имеющих доступ к защищаемой информации;

- всех структурных и обособленных подразделений органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»;

- подведомственные муниципальные учреждения и предприятия органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»;

- третьих лиц (поставщиков, подрядчиков, провайдеров услуг), привлекаемых к выполнению работ или оказанию услуг, связанных с разработкой, эксплуатацией, сопровождением ИС или получением доступа к защищаемой информации.

Требования настоящей Политики подлежат обязательному включению в договоры, государственные и муниципальные контракты и технические задания, заключаемые с третьими лицами.

3.6. Требования настоящей Политики применяются на всех этапах жизненного цикла ИС, подпадающих под ее действие, включая проектирование, разработку, внедрение, эксплуатацию, модернизацию и вывод из эксплуатации, в объеме, соответствующем категории ИС, уровню ее защищенности и значимости обрабатываемой информации.

4. Цели и задачи защиты информации

4.1. Основными целями являются:

а) обеспечение защиты информации ограниченного доступа, персональных данных и иной защищаемой информации, обрабатываемой в ИС Центра, от актуальных внутренних и внешних угроз, включая умышленные и непреднамеренные действия работников органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» и третьих лиц;

б) обеспечение конфиденциальности, целостности и доступности информации во всех ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», подпадающих под действие настоящей Политики, с учетом значимости обрабатываемой информации и возможных последствий нарушения ее безопасности;

в) обеспечение устойчивости функционирования ИС на всех этапах их жизненного цикла и предотвращение существенных негативных последствий для деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», обусловленных нарушением конфиденциальности, целостности или доступности защищаемой информации;

г) недопущение возникновения существенного ущерба для деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» в результате нарушения безопасности информации;

д) соблюдение требований законодательства Российской Федерации и нормативных

правовых актов уполномоченных органов в области защиты информации.

4.2. Для достижения указанных целей в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» решаются следующие задачи:

а) классификация информационных активов и категорирование ИС в соответствии с приказом ФСТЭК России от 11 апреля 2025 г. № 117;

б) оценка рисков информационной безопасности и определение уровней защищенности ИС в целях выбора адекватных мер защиты информации;

в) реализация организационных и технических мер защиты информации в соответствии с установленными уровнями защищенности;

г) обеспечение физической и логической защищенности информационной инфраструктуры;

д) управление доступом к информации и ИС на основе принципа минимально необходимых полномочий;

е) регистрация и мониторинг событий информационной безопасности, выявление и реагирование на инциденты;

ж) обеспечение непрерывности деятельности органов местного самоуправления путем резервного копирования и восстановления информационных ресурсов;

з) повышение осведомленности и квалификации работников в области информационной безопасности;

и) защита деловой репутации и имиджа органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» путем предотвращения утечек информации и нарушений ее безопасности.

4.3. Оценка эффективности системы защиты информации осуществляется на основе показателей ее состояния, рассчитываемых в соответствии с Методикой оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации, утвержденной ФСТЭК России 2 мая 2024 г. Периодичность оценки устанавливается в зависимости от категории ИС, но не реже одного раза в шесть месяцев.

4.4. Минимально необходимый уровень защиты информации должен соответствовать составу мер, реализация которых предусмотрена нормативными правовыми актами Российской Федерации, и быть достаточным для нейтрализации типовых актуальных угроз безопасности информации.

5. Принципы защиты информации

Органы местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» в своей деятельности по защите информации руководствуется следующими принципами:

а) **Законность -** все мероприятия по защите информации осуществляются в соответствии с законодательством Российской Федерации, нормативными правовыми актами уполномоченных органов и муниципальными правовыми актами;

б) **Риск-ориентированный подход и соразмерность мер -** меры защиты информации определяются с учетом значимости обрабатываемой информации, категории ИС и возможных последствий нарушения ее безопасности, без применения избыточных мер, не обусловленных реальными рисками;

в) **Комплексность –** защита информации обеспечивается путем применения взаимодополняющих организационных, технических и физических мер, охватывающих все этапы жизненного цикла ИС и возможные каналы реализации угроз;

г) **Системность и управляемость –** система защиты информации формируется как совокупность взаимосвязанных процессов, мер и средств, управление которыми осуществляется централизованно на основе установленных полномочий и ответственности;

д) **Непрерывность защиты** – обеспечение защиты информации на всех этапах жизненного цикла ИС: проектирование, разработка, внедрение, эксплуатация, модернизация и

вывод из эксплуатации;

е) **Минимально необходимые полномочия и разделение ответственности** – доступ к информации и ИС предоставляется пользователям в объеме, необходимом для выполнения их должностных обязанностей, с разграничением функций и ответственности, в том числе при выполнении административных операций;

ж) **Контролируемость и подотчетность –** деятельность по защите информации подлежит контролю и оценке, включая регистрацию значимых событий информационной безопасности и анализ результатов реализуемых мер;

з) **Персональная ответственность –** работники органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» несут персональную ответственность за соблюдение требований настоящей Политики и требований по защите информации в пределах предоставленных им полномочий и должностных обязанностей;

и) **Своевременное реагирование и восстановление –** выявление, анализ и реагирование на инциденты информационной безопасности, а также принятие мер по восстановлению функционирования ИС и предотвращению повторных нарушений;

к) **Непрерывное совершенствование –** система защиты информации подлежит регулярной оценке и совершенствованию с учетом изменений угроз, архитектуры ИС и требований законодательства Российской Федерации.

6. Объекты защиты информации

6.1. Объектами защиты информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» являются ИС и связанные с ними компоненты, подпадающие под действие раздела 3 настоящей Политики, а также информация, обрабатываемая в указанных ИС.

6.2. К объектам защиты информации относятся:

а) информационные системы, включая:

- иные ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», подлежащие защите в соответствии с приказом ФСТЭК России от 11 апреля 2025 г. № 117;
- ИС, отнесенные к объектам критической информационной инфраструктуры Российской Федерации в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ;
- автоматизированные рабочие места пользователей, являющиеся компонентами ИС.

б) информация, обрабатываемая в ИС, включая:

- информацию ограниченного доступа (не составляющую государственную тайну);
- персональные данные;
- иную защищаемую информацию, подлежащую защите в соответствии с законодательством Российской Федерации и муниципальными правовыми актами;

в) технические средства обработки информации, включая:

- серверное оборудование;
- средства коммутации и маршрутизации;
- средства межсетевого экранирования и обнаружения/предотвращения вторжений;
- СКЗИ, сертифицированные ФСБ России;
- персональные компьютеры, ноутбуки, планшетные устройства и иные средства вычислительной техники, используемые для обработки защищаемой информации;

г) программное обеспечение, включая:

- операционные системы;
- системы управления базами данных;
- прикладное программное обеспечение, используемое для обработки защищаемой информации;
- средства защиты информации (СЗИ), в том числе антивирусные средства, средства контроля целостности и средства аудита;

д) информационно-телекоммуникационная инфраструктура, включая:

- локальные вычислительные сети органов местного самоуправления муниципального

образования «Городской округ Бердянск Запорожской области»;

- межсетевые экраны и сегменты сети, разделяющие зоны доверия;
- каналы связи с внешними организациями и провайдерами услуг;
- беспроводные сети передачи данных (Wi-Fi);

е) носители информации, включая:

- электронные носители (жесткие диски, твердотельные накопители, оптические диски, флэш-накопители);
- бумажные носители, содержащие информацию ограниченного доступа или персональные данные.

6.3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ) органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» осуществляется в соответствии с Положением о системе обеспечения безопасности значимых объектов критической информационной инфраструктуры, которое развивает и конкретизирует требования настоящей Политики в части защиты ЗОКИИ.

Ознакомление с информацией, содержащейся в документах системы безопасности ЗОКИИ, допускается только для работников органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», чьи должностные обязанности непосредственно связаны с эксплуатацией, сопровождением или обеспечением безопасности ЗОКИИ, в объеме, необходимом для выполнения ими трудовых функций.

6.4. К объектам защиты также относятся процессы и процедуры обработки информации в ИС, включая процессы:

а) идентификации и аутентификации пользователей;
б) резервного копирования и восстановления данных;
в) управления учетными записями и правами доступа;
г) реагирования на инциденты информационной безопасности

6.5. Объекты защиты информации подлежат учету и классификации с учетом категории ИС, уровня ее защищенности и значимости обрабатываемой информации в порядке, установленном настоящей Политикой и муниципальными правовыми актами.

6.6. Объекты защиты информации, эксплуатация или обслуживание которых осуществляется с привлечением третьих лиц, подлежат защите в объеме, определенном договорами и техническими заданиями, с учетом требований настоящей Политики.

7. Основные угрозы безопасности информации

7.1. Угрозы безопасности информации, актуальные для органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», определяются с учетом особенностей их деятельности, архитектуры ИС, значимости обрабатываемой информации и возможных последствий нарушения ее конфиденциальности, целостности и доступности.

Перечень угроз, приведенный в настоящем разделе, носит общий характер и не является исчерпывающим. Актуальные угрозы для конкретных ИС уточняются при их категорировании и разработке моделей угроз в установленном порядке.

7.2. К основным угрозам относятся:

7.2.1. **Угрозы, реализуемые внешними нарушителями:**

а) несанкционированный доступ к информации и ИС из внешних сетей, включая компрометацию учетных данных и эксплуатацию уязвимостей программного обеспечения и средств защиты информации;

б) сетевые атаки на информационную инфраструктуру, включая атаки, направленные на нарушение доступности ИС и сетевых сервисов;

в) распространение вредоносного программного обеспечения, приводящее к нарушению функционирования ИС или компрометации информации;

г) целевые воздействия на работников органов местного самоуправления

муниципального образования «Городской округ Бердянск Запорожской области» с использованием методов социальной инженерии.

7.2.2. **Угрозы, реализуемые внутренними нарушителями:**

а) несанкционированный доступ к информации и ИС работниками органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» или третьими лицами, имеющими легальный доступ, включая превышение предоставленных полномочий и использование учетных записей иных лиц;

б) несанкционированные действия с информацией, включая копирование, модификацию, уничтожение или использование информации в личных целях;

в) несанкционированные изменения конфигураций ИС, программного обеспечения и средств защиты информации.

7.2.3. **Угрозы, связанные с уязвимостями информационных систем:**

а) эксплуатация уязвимостей программного обеспечения и технических средств в результате несвоевременного обновления, использования устаревших или неподдерживаемых компонентов;

б) недостаточная защищенность конфигураций ИС, включая избыточные привилегии и отсутствие сегментации.

7.2.4. **Угрозы технического характера:**

а) отказы и сбои технических средств, систем электропитания и каналов связи;

б) повреждение или утрата носителей информации;

в) ошибки эксплуатации и технического обслуживания ИС.

7.2.5. **Угрозы, связанные с недостатками организационных мер:**

а) недостаточная эффективность контроля доступа и управления учетными записями;

б) несвоевременное аннулирование прав доступа при изменении кадрового состава;

в) недостаточная осведомленность работников в области информационной безопасности;

г) отсутствие или несвоевременная актуализация внутренних регламентов и процедур.

7.3. Для ИС, отнесенных к значимым объектам критической информационной инфраструктуры Российской Федерации, дополнительно учитываются угрозы компьютерных инцидентов в соответствии с требованиями законодательства Российской Федерации и нормативными правовыми актами уполномоченных органов.

7.4. Оценка актуальности и значимости угроз для каждой ИС осуществляется при ее категорировании и при разработке модели угроз для конкретной системы в порядке, установленном муниципальными нормативными правовыми актами.

8. Категорирование информационных систем и уровни защищенности

8.1. Все ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», подпадающие под действие раздела 3 настоящей Политики, подлежат обязательному категорированию в порядке, установленном приказом ФСТЭК России от 11 апреля 2025 г. № 117.

8.2. Категорирование ИС осуществляется в целях определения значимости обрабатываемой информации и возможных последствий нарушения ее конфиденциальности, целостности и доступности для деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», интересов работников, контрагентов и выполнения возложенных функций.

8.3. В рамках настоящей Политики под категорией ИС понимается классификационная характеристика, определяемая в соответствии с приказом ФСТЭК России от 11 апреля 2025 г. № 117 и отражающая значимость обрабатываемой в ИС информации, а также возможные последствия нарушения ее конфиденциальности, целостности и доступности.

Категория ИС используется в качестве основания для отнесения ИС к соответствующему классу защищенности и установления уровня защищенности, определяющего совокупность обязательных требований и мер по защите информации, подлежащих реализации в данной ИС.

8.4. Категорирование ИС проводится комиссией, формируемой распоряжением Администрации Бердянского городского округа. В состав комиссии включаются заместители

главы Администрации Бердянского городского округа, работники структурных подразделений в области информационной безопасности и информационных технологий, иные должностные лица органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

Результаты категорирования оформляются протоколами и подлежат утверждению в установленном порядке.

8.5. При категорировании ИС учитываются:

а) вид и значимость обрабатываемой информации (персональные данные, информация ограниченного доступа, иная защищаемая информация);

б) архитектура и назначение ИС;

в) возможные последствия нарушения конфиденциальности, целостности и доступности информации;

г) принадлежность ИС к объектам критической информационной инфраструктуры Российской Федерации (при наличии).

8.6. По результатам категорирования каждой ИС устанавливается уровень защищенности, определяющий:

а) состав обязательных требований по защите информации;

б) перечень организационных и технических мер защиты;

в) требования к применяемым средствам защиты информации;

г) периодичность оценки состояния защищенности.

8.7. Категория и уровень защищенности ИС подлежат пересмотру:

а) при вводе в эксплуатацию новой ИС;

б) при изменении состава, объема или категории обрабатываемой информации;

в) при изменении архитектуры или назначения ИС;

г) при изменении статуса ИС в части отнесения к объектам критической информационной инфраструктуры;

д) не реже одного раза в три года.

8.8. В целях обеспечения управляемости и актуальности сведений о категорировании ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», в составе настоящей Политики приводится шаблон перечня ИС с указанием категории и уровня защищенности (приложение № 1 к настоящей Политике).

Фактический перечень ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» с указанием их категории и уровня защищенности оформляется в виде отдельного документа, утверждается распоряжением Администрации Бердянского городского округа и относится к информации ограниченного распространения. Доступ к указанному документу предоставляется в установленном порядке ограниченному кругу лиц, в пределах их должностных обязанностей.

Актуализация фактического перечня ИС осуществляется по мере необходимости без внесения изменений в текст настоящей Политики.

9. Организация управления защитой информации

9.1. Общее руководство и ответственность за организацию защиты информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» осуществляет Глава Бердянского городского округа в соответствии с законодательством Российской Федерации.

Глава Бердянского городского округа обеспечивает утверждение Политики защиты информации, внутренних нормативных документов в области информационной безопасности, а также выделение необходимых организационных, кадровых и финансовых ресурсов для реализации мероприятий по защите информации.

9.2. Организация и координация деятельности по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» возлагаются на должностное лицо, назначаемое распоряжением

Администрации Бердянского городского округа и ответственное за обеспечение защиты информации.

Указанное должностное лицо осуществляет свои функции в соответствии с требованиями законодательства Российской Федерации и нормативных правовых актов в области информационной безопасности, включая приказ ФСТЭК России от 11 апреля 2025 г. № 117, и подчиняется непосредственно Главе Бердянского городского округа.

Должностное лицо, ответственное за обеспечение защиты информации:

- организует выполнение требований законодательства Российской Федерации и нормативных правовых актов в области защиты информации, включая приказ ФСТЭК России от 11 апреля 2025 г. № 117;

- координирует деятельность структурных и обособленных подразделений органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» по вопросам защиты информации;

- организует категорирование ИС и пересмотр их категории и уровня защищенности;

- обеспечивает взаимодействие с уполномоченными государственными органами по вопросам информационной безопасности в пределах своей компетенции.

9.3. Функции по методическому обеспечению, контролю и координации мероприятий по защите информации возлагаются на структурное подразделение Администрации Бердянского городского округа, уполномоченное в области защиты информации (схема управления системой защиты информации приведена в приложение № 2 к настоящей Политике).

Уполномоченное структурное подразделение Администрации Бердянского городского округа:

а) разрабатывает и актуализирует Политику защиты информации и внутренние регламенты;

б) осуществляет контроль соблюдения требований информационной безопасности;

в) организует учет, анализ и первичную обработку инцидентов информационной безопасности;

г) участвует в оценке состояния защищенности ИС;

д) готовит предложения по совершенствованию системы защиты информации.

9.4. Техническая реализация мер защиты информации, эксплуатация и сопровождение ИС, а также средств защиты информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» осуществляются отделом информационных технологий, а в обособленных подразделениях — специалистами, ответственными за информационные технологии, в пределах их полномочий.

Структурное подразделение Администрации Бердянского городского округа, ответственное за информационные технологии:

а) обеспечивает функционирование, техническую эксплуатацию и сопровождение ИС органов местного самоуправления;

б) реализует технические меры защиты информации в соответствии с требованиями настоящей Политики, внутренних регламентов и решений, принятых уполномоченным подразделением в области информационной безопасности;

в) участвует в выявлении и устранении уязвимостей ИС, а также в восстановлении их работоспособности при нарушениях функционирования;

г) обеспечивает выполнение требований по резервному копированию и восстановлению информации в ИС в установленном порядке.

9.5. Руководители структурных и обособленных подразделений органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» несут ответственность за соблюдение требований по защите информации в пределах деятельности соответствующих подразделений, включая:

а) обеспечение выполнения требований настоящей Политики работниками подразделения;

б) контроль использования ИС и информации в служебных целях;

в) своевременное информирование о выявленных инцидентах информационной

безопасности.

9.6. Работники, эксплуатирующие ИС или имеющие доступ к защищаемой информации, несут персональную ответственность за:

а) соблюдение требований настоящей Политики и внутренних регламентов в области защиты информации;

б) использование ИС и защищаемой информации только в целях, соответствующих их должностным обязанностям;

в) соблюдение правил работы с учетными записями, средствами аутентификации и носителями информации;

г) немедленное информирование руководителя подразделения или отдела информационных технологий о подозрительных событиях, фактах несанкционированного доступа или инцидентах информационной безопасности.

9.7. Третьи лица (подрядчики, поставщики, сервисные организации и иные контрагенты), привлекаемые к работам (оказанию услуг), связанным с доступом к ИС или информации органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», обязаны соблюдать требования по защите информации в объеме, установленном договорами (контрактами), техническими заданиями и приложениями о конфиденциальности.

Контроль соблюдения третьими лицами требований по защите информации, включая требования к обработке персональных данных, осуществляется в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»» и приказом ФСТЭК России от 11 апреля 2025 г. №117.

Ответственность за:

а) включение требований по защите информации в проекты договоров и технические задания возлагается на руководителя подразделения-инициатора;

б) организация контроля фактического соблюдения требований третьими лицами в ходе выполнения работ возлагается на руководителя структурного подразделения Администрации Бердянского городского округа, выступившего инициатором заключения договора (заказчиком работ), при методическом руководстве и координации со стороны отдела информационных технологий.

9.8. Взаимодействие подразделений органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

Порядок взаимодействия структурных и обособленных подразделений органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» по защите информации регламентируется приложением № 3 к настоящей Политике.

9.9. В соответствии с пунктом 25 приказа ФСТЭК России от 11 апреля 2025 г. № 117 в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» разрабатываются и утверждаются внутренние стандарты и регламенты по защите информации.

Внутренние стандарты и регламенты утверждаются постановлением Администрации Бердянского городского округа (перечень внутренних стандартов и регламентов приведен в приложении № 4 к настоящей Политике).

10. Основные требования по защите информации

10.1. Защита информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» обеспечивается в ИС, подпадающих под действие настоящей Политики, с учетом их категории, уровня защищенности, значимости обрабатываемой информации и возможных последствий нарушения ее безопасности.

10.2. В целях обеспечения защиты информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» реализуются следующие основные требования:

а) организационные требования, включая:

- установление ролей, полномочий и ответственности в области информационной безопасности;

- разработку, утверждение и актуализацию внутренних нормативных документов по защите информации;

- организацию обучения и повышения осведомленности работников в области информационной безопасности;

б) требования по управлению доступом, включая:

- предоставление доступа к информации и ИС на основе принципа минимально необходимых полномочий;

- использование персональных учетных записей;

- своевременное изменение и аннулирование прав доступа;

в) требования по защите информации от вредоносного программного обеспечения, включая применение средств защиты информации и организационных мер, направленных на предотвращение, выявление и нейтрализацию вредоносных воздействий;

г) требования по обеспечению целостности и доступности информации, включая:

- защиту от несанкционированного изменения и уничтожения информации;

- обеспечение резервного копирования и восстановления информации;

- принятие мер по обеспечению устойчивости функционирования ИС;

д) требования по защите сетевого взаимодействия и каналов связи, включая контроль сетевых соединений и защиту передачи информации;

е) требования по регистрации и анализу событий информационной безопасности, включая выявление и реагирование на инциденты информационной безопасности;

ж) требования по управлению уязвимостями и обновлениями, включая учет уязвимостей и контроль актуальности программного обеспечения и средств защиты информации;

з) требования по физической защите, включая защиту помещений, технических средств и носителей информации;

и) требования по обеспечению информационной безопасности при взаимодействии с третьими лицами, включая установление соответствующих требований в договорах и технических заданиях.

10.3. Конкретный состав и объем мер защиты информации, реализуемых в ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», определяется в зависимости от категории ИС и уровня ее защищенности в соответствии с требованиями законодательства Российской Федерации, нормативных правовых актов уполномоченных органов и внутренних стандартов и регламентов органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» (основные ориентировочные требования и целевые показатели по обеспечению защиты информации указаны в приложении № 5 к настоящей Политике).

10.4. Детализация требований по защите информации, порядок реализации мер, а также распределение ответственности за их выполнение устанавливаются во внутренних стандартах, регламентах и инструкциях органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», утверждаемых в установленном порядке.

11. Порядок утверждения, внесения изменений и актуализации Политики

11.1. Настоящая Политика утверждается постановлением Администрации Бердянского городского округа.

11.2. Изменения и дополнения в настоящую Политику вносятся на основании решения Главы Бердянского городского округа и утверждаются постановлением Администрации Бердянского городского округа.

11.3. Актуализация настоящей Политики осуществляется при необходимости, в том числе в случаях:

а) изменения законодательства Российской Федерации и нормативных правовых актов уполномоченных органов в области информационной безопасности;

б) изменения структуры органов местного самоуправления муниципального образования

«Городской округ Бердянск Запорожской области», состава или архитектуры ИС, подпадающих под действие настоящей Политики;

в) изменения подходов к обеспечению защиты информации либо выявления существенных недостатков в системе защиты информации;

г) по результатам проверок, оценок состояния защищенности или инцидентов информационной безопасности.

11.4. Контроль актуальности настоящей Политики осуществляется должностным лицом, ответственным за обеспечение информационной безопасности.

11.5. Настоящая Политика доводится до сведения работников органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» в части, касающейся их должностных обязанностей, в установленном порядке.

12. Ответственность за нарушение требований настоящей Политики

12.1. Работники органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», виновные в нарушении требований настоящей Политики, несут ответственность в соответствии с законодательством Российской Федерации, муниципальными нормативными актами органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» и условиями трудовых договоров в пределах предоставленных им полномочий и должностных обязанностей,

12.2. Руководители структурных и обособленных подразделений органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» несут ответственность за организацию выполнения требований по защите информации в подчиненных подразделениях, а также за своевременное принятие мер по устранению выявленных нарушений.

12.3. Должностное лицо, ответственное за обеспечение защиты информации, несет ответственность за организацию и координацию деятельности по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» в пределах своей компетенции.

12.4. Третьи лица (подрядчики, поставщики, иные организации), привлекаемые к выполнению работ или оказанию услуг с доступом к ИС или информации органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области», несут ответственность за соблюдение требований по защите информации в соответствии с условиями заключенных договоров и требованиями законодательства Российской Федерации.

12.5. Факт нарушения требований настоящей Политики подлежит рассмотрению в установленном порядке с учетом характера нарушения, причин его возникновения и возможных последствий для деятельности органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области».

Приложение № 1 к Политике по защите информации
в органах местного самоуправления
муниципального образования «Городской округ
Бердянск Запорожской области»

Шаблон перечня информационных систем органов местного самоуправления
муниципального образования «Городской округ Бердянск Запорожской области» с указанием категории и уровня защищенности

Фактический перечень ИС органов местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области» с указанием их категории и уровня защищенности оформляется в виде отдельного документа, утверждается распоряжением Администрации Бердянского городского округа, относится к информации ограниченного распространения и не включается в состав настоящей Политики.

№ п/п	Наименование информационной системы	Владелец ИС	Назначение ИС (подразделение)	Категория ИС[1]	Уровень защищенности[2]	Примечание
1	Система электронного документооборота (СЭД) Пример заполнения; перечень не является фактическим	Автоматизация документооборота	Центр	К2	У32	

[1] *Категория ИС определяется в соответствии с приказом ФСТЭК России от 11.04.2025 №117 на основе оценки значимости обрабатываемой информации и потенциальных последствий нарушения ее безопасности.*

[2] *Уровень защищенности определяет совокупность обязательных требований к защите информации, перечень СЗИ и периодичность оценки состояния защищенности.*

* Примечания:

1. Перечень подлежит актуализации при:
- вводе в эксплуатацию новых ИС;
- изменении категории или уровня защищенности существующих ИС;
- изменении принадлежности ИС к значимым объектам КИИ.

2. Актуализация Перечня осуществляется правовым актом администрации без переутверждения Политики по защите информации.
3. Ответственность за ведение и актуализацию Перечня возложена на должностное лицо, ответственное за обеспечение защиты информации.

Приложение № 2 к Политике по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ
и порядок оценки состояния защищенности

1. Этапы управления защитой информации

Деятельность по защите информации в органах местного самоуправления осуществляется в рамках непрерывного цикла, включающего четыре этапа:

Этап	Основные действия	Ответственное подразделение
1. Разработка и планирование	- Определение событий в ИС, наступление которых может привести к нарушению целей защиты информации; - Идентификация ИС, программных и программно-аппаратных средств, - Несанкционированный доступ, к которым может нарушить цели защиты; - Выявление и оценка угроз безопасности информации; - Планирование мер защиты и оценка необходимых ресурсов.	Отдел информационных технологий
2. Проведение мероприятий	-Реализация запланированных мер защиты; -Техническая настройка и эксплуатация СЗИ; -Обучение персонала; -Контроль выполнения мероприятий.	Отдел информационных технологий
3. Оценка состояния защиты	-Проведение оценки показателей состояния защиты информации; -Анализ эффективности реализованных мер; -Формирование отчета о состоянии защищенности.	Отдел информационных технологий
4. Совершенствование	- Анализ результатов оценки; - Разработка плана мероприятий по улучшению защиты; - Корректировка регламентов и стандартов.	Отдел информационных технологий при участии подразделений-эксплуатантов ИС

2. Порядок оценки состояния защищенности

2.1. Оценка состояния защиты информации проводится на основе показателя, характеризующего текущее состояние защиты информации от актуальных угроз безопасности информации.

2.2. Показатели состояния защиты информации являются ключевыми показателями эффективности деятельности по защите информации.

2.3. Периодичность проведения оценки:

- плановая - не реже одного раза в шесть месяцев для всех ИС категории 2 и выше; для ИС категории 3 - не реже одного раза в год;

- внеочередная - в случаях:

а) возникновения инцидента ИБ, повлекшего наступление негативных последствий (значимый инцидент);

б) изменения архитектуры ИС или ее категории; -

в) запроса руководителя органа местного самоуправления о текущем значении показателя защищенности;

г) запроса ФСТЭК России или Минобрнауки России.

2.4. Результаты оценки доводятся до сведения руководителя органа местного самоуправления. При несоответствии показателей установленным нормам отдел информационных технологий представляет информацию с предложением о необходимости совершенствования системы защиты информации.

2.5. По указанию руководителя органа местного самоуправления отдел информационных технологий разрабатывает план мероприятий по улучшению защиты информации совместно со структурными (обособленными) подразделениями, эксплуатирующими ИС и обеспечивающими ее функционирование.

3. Обоснование ресурсов для защиты информации

Отдел информационных технологий своевременно разрабатывает и представляет руководителю органа местного самоуправления обоснованные предложения о ресурсах, необходимых для проведения мероприятий по защите информации. В обоснование включаются:

- цели защиты информации;
- показатели эффективности, для достижения которых требуются ресурсы;
- прогнозируемые негативные последствия (ущерб), которые могут наступить в случае отказа в выделении ресурсов.

Приложение № 3 к Политике по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ АДМИНИСТРАЦИИ БЕРДЯНСКОГО ГОРОДСКОГО ОКРУГА

Подразделение / Должностное лицо	**Основные функции**
Глава Бердянского городского округа	- Несет общую ответственность за организацию защиты информации в Администрации Бердянского городского округа; - Утверждает Политику по защите информации и внутренние регламенты; - Обеспечивает выделение финансовых, кадровых и технических ресурсов; - Назначает должностное лицо, ответственное за ЗИ.
Должностное лицо, ответственное за обеспечение защиты информации	- Координирует деятельность всех подразделений по обеспечению ИБ; - Организует категорирование ИС и установление уровней защищенности; - Организует подготовку и согласование внутренних регламентов и стандартов; - Обеспечивает взаимодействие с ФСТЭК России, ФСБ России, Национальным координационным центром по компьютерным инцидентам (НКЦКИ).
Отдел информационных технологий	- Реализация Политики по защите информации; - Определение требований к защите информации; - Координация мероприятий по защите информации во всех подразделениях; - Контроль и оценка эффективности мер и средств защиты; - Методическая помощь работникам по вопросам защиты информации; - Регулярная оценка и управление рисками ИБ; - Выбор и внедрение СЗИ и СКЗИ; - Обеспечение минимально необходимого доступа к ИС; - Обучение и повышение квалификации работников в сфере защиты информации; - Расследование инцидентов ИБ; - Взаимодействие с НКЦКИ по вопросам КИИ. - Техническая реализация мер защиты информации; - Эксплуатация и сопровождение СЗИ; - Централизованное управление конфигурациями ИС и ПО; - Выявление и устранение уязвимостей; - Резервное копирование и восстановление информации; - Регистрация событий ИБ и обеспечение функционирования системы мониторинга; - Техническая поддержка реализации требований Политики ИБ.

Руководители структурных и обособленных подразделений администрации	- Обеспечение соблюдения требований Политики по защите информации в подразделении; - Контроль надлежащего использования ИС и защищаемой информации работниками; - Своевременное информирование отдела комплексной безопасности о выявленных инцидентах ИБ и нарушениях.
Работники администрации	- Соблюдение требований Политики по защите информации и внутренних регламентов - Надлежащее использование ИС и защищаемой информации в рамках должностных обязанностей; - Немедленное информирование руководителя структурного подразделения или отдела информационных технологий о

Приложение № 4 к Политике по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

ПЕРЕЧЕНЬ
внутренних регламентов и стандартов в области защиты информации

№ п/п	Наименование документа	Основное содержание	Периодичность актуализации
1	Регламент обеспечения защиты информации на стадиях жизненного цикла ИС	Порядок реализации мер защиты на этапах: проектирование, разработка, внедрение, эксплуатация, модернизация, вывод из эксплуатации	Не реже 1 раза в 2 года
2	Регламент предоставления удаленного доступа к ИС	Порядок предоставления удаленного доступа работникам администрации и лицам, не являющимся работниками администрации (включая аутентификацию, авторизацию, учет сессий)	Не реже 1 раза в 2 года
3	Регламент взаимодействия с подрядными организациями	Порядок предоставления доступа к ИС подрядным организациям и (или) передачи им информации, содержащейся в ИС	Не реже 1 раза в 2 года
4	Регламент обращения с информацией ограниченного доступа и ее носителями	Порядок работы с информацией, для которой в соответствии с Федеральными законами установлены требования к обеспечению конфиденциальности, и ее носителями (включая хранение, передачу, уничтожение)	Не реже 1 раза в 2 года
5	Регламент доступа работников к сети «Интернет» и внешним сетям	Порядок доступа работников к сети «Интернет» и ее использования, взаимодействия с иными внешними информационно-телекоммуникационными сетями и ИС	Не реже 1 раза в 2 года
6	Регламент обучения и повышения осведомленности в области информационной безопасности	Порядок обучения работников, включая первичный инструктаж, периодическое обучение, специализированное обучение для ответственных лиц	Ежегодно
7	Регламент выявления, оценки и устранения	Порядок проведения сканирования уязвимостей,	Ежегодно

	уязвимостей ИС	оценки критичности, планирования и контроля устранения	
8	Регламент обновления программного обеспечения	Порядок контроля своевременности установки обновлений и исправлений безопасности для операционных систем, прикладного ПО и СЗИ	Ежегодно
9	Регламент предоставления внешних сервисов	Порядок предоставления внутренним и внешним пользователям сервисов, доступ к которым осуществляется с использованием сети «Интернет» (веб-порталы, API и др.)	Не реже 1 раза в 2 года
10	Регламент мониторинга информационной безопасности	Порядок сбора, регистрации, анализа и хранения событий ИБ; определение пороговых значений для выявления инцидентов	Ежегодно
11	Регламент инвентаризации ИС и управления конфигурацией	Порядок проведения инвентаризации ИС, ведения базы конфигураций, контроля несанкционированных изменений	Ежегодно
12	Регламент управления учетными записями	Порядок заведения, контроля, блокирования и аннулирования учетных записей пользователей и средств аутентификации в ИС	Ежегодно
13	Регламент администрирования ИС	Порядок выполнения административных операций, разделение привилегированных функций, регистрация действий администраторов	Ежегодно
14	Регламент контроля уровня защищенности ИС	Порядок проведения оценки состояния защищенности, расчета показателей, формирования плана мероприятий по устранению выявленных нарушений	В соответствии с разделом 5 Политики
15	Регламент обеспечения сетевой безопасности	Порядок разделения инфраструктуры на зоны доверия, настройки межсетевых экранов, изоляции критичных систем и резервных копий; план-график поэтапной реализации для существующих систем	Не реже 1 раза в 2 года
16	Стандарт первичной идентификации пользователей	Требования к процедуре первичной идентификации, верификации личности, формированию учетных данных	Ежегодно
17	Стандарт конфигурации и настройки ПО и ПАК	Требования к безопасным конфигурациям операционных систем, СУБД, прикладного ПО и программно-аппаратных	Ежегодно

		комплексов	
18	Стандарт защиты средств вычислительной техники с доступом в Интернет	Требования к защите АРМ внутренних пользователей, имеющих постоянный доступ к сети «Интернет» (антивирусная защита, СКЗИ, настройки брандмауэра)	Ежегодно
19	Стандарт сбора и анализа событий ИБ	Требования к формату, полноте и периодичности сбора событий, связанных с нарушением безопасности информации или функционирования ИС	Ежегодно
20	Стандарт моделей доступа пользователей	Требования к применяемым моделям разграничения доступа (ролевой, мандатный, дискреционный), правилам назначения прав	Ежегодно

Примечания:

1. Регламенты и стандарты утверждаются правовым актом Администрации Бердянского городского округа.
2. Документы доводятся до сведения всех работников Администрации Бердянского городского округа, а также подрядных организаций в части, их касающейся.
3. Актуализация перечня осуществляется при вступлении в силу новых требований законодательства или изменении организационной структуры Администрации Бердянского городского округа.

Приложение № 5 к Политике по защите информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

Основные ориентировочные требования и целевые показатели по обеспечению защиты информации в органах местного самоуправления муниципального образования «Городской округ Бердянск Запорожской области»

1. Общие положения

1.1. Настоящее приложение устанавливает ориентировочные требования и целевые показатели по обеспечению защиты информации в ИС органах местного самоуправления, подпадающих под действие настоящей Политики.

1.2. Конкретный состав, объем, сроки и порядок реализации мероприятий по защите информации определяются во внутренних стандартах и регламентах с учетом категории ИС, уровня ее защищенности, значимости обрабатываемой информации, а также технических и организационных возможностей органов местного самоуправления.

1.3. Требования и показатели, приведенные в настоящем приложении, применяются дифференцированно, в зависимости от категории ИС и не подлежат автоматическому распространению на все ИС органов местного самоуправления в одинаковом объеме.

2. Управление доступом

2.1. Доступ пользователей к ИС и информации должен предоставляться на основе принципа минимально необходимых полномочий.

2.2. Использование общих (групповых) учетных записей не допускается, за исключением случаев, обоснованных технологической необходимостью и оформленных в установленном порядке.

2.3. Изменение, приостановление и аннулирование прав доступа пользователей должно осуществляться своевременно, в том числе при изменении должностных обязанностей или прекращении трудовых отношений.

2.4. Учетные записи пользователей, не используемые в течение установленного регламентами периода, подлежат блокированию или удалению.

3. Защита от вредоносного программного обеспечения

3.1. В ИС органов местного самоуправления должны применяться средства и организационные меры защиты от вредоносного программного обеспечения в соответствии с установленными требованиями.

3.2. Обновление средств защиты информации и антивирусных баз должно осуществляться регулярно, с учетом категории ИС и критичности обрабатываемой информации.

3.3. Реагирование на выявленные факты заражения вредоносным программным обеспечением осуществляется в установленном порядке с приоритетом обеспечения устойчивости функционирования ИС.

4. Управление уязвимостями и обновлениями

4.1. В ИС органов местного самоуправления должен обеспечиваться учет уязвимостей программного обеспечения и технических средств.

4.2. Установка обновлений безопасности и исправлений уязвимостей осуществляется в приоритетном порядке для ИС, нарушение безопасности которых может повлечь существенные негативные последствия.

4.3. Сроки устранения уязвимостей и внедрения обновлений определяются во внутренних регламентах с учетом категории ИС и оценки рисков информационной безопасности.

5. Обеспечение целостности и доступности информации

5.1. Для ИС органов местного самоуправления должны быть предусмотрены меры, направленные на предотвращение несанкционированного изменения, уничтожения или блокирования информации.

5.2. Резервное копирование информации должно осуществляться в объемах и с периодичностью, достаточными для восстановления функционирования ИС в случае сбоев или инцидентов информационной безопасности.

5.3. Порядок хранения резервных копий и восстановления информации определяется внутренними регламентами с учетом категории ИС.

6. Регистрация и анализ событий информационной безопасности

6.1. В ИС органов местного самоуправления должна обеспечиваться регистрация значимых событий информационной безопасности, связанных с нарушением безопасности информации или функционирования ИС.

6.2. Анализ событий информационной безопасности осуществляется с периодичностью и в объеме, определяемых внутренними регламентами, с учетом категории ИС и уровня ее защищенности.

6.3. Выявленные инциденты информационной безопасности подлежат регистрации, анализу и реагированию в установленном порядке.

7. Физическая защита и защита носителей информации

7.1. Доступ к помещениям, в которых размещены технические средства обработки информации и носители информации, должен быть ограничен и контролируем.

7.2. Носители информации, содержащие защищаемую информацию, подлежат учету, хранению и уничтожению в установленном порядке.

8. Защита информации при взаимодействии с третьими лицами

8.1. При привлечении третьих лиц к работам или услугам, связанным с доступом к ИС или информации органов местного самоуправления, должны устанавливаться требования информационной безопасности, соответствующие категории ИС.

8.2. Требования по защите информации включаются в договоры, технические задания и иные документы, регулирующие взаимодействие с третьими лицами.

9. Заключительные положения

9.1. Реализация требований и целевых показателей, установленных настоящим приложением, подлежит контролю и уточнению в рамках функционирования системы защиты информации в органах местного самоуправления.

9.2. Настоящее приложение применяется в совокупности с настоящей Политикой защиты информации и внутренними нормативными документами в области защиты информации в органах местного самоуправления.