ГЛАВА ВЕРХНЕУСЛОНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ ЮГАРЫ ОСЛАН МУНИЦИПАЛЬ РАЙОНЫ БАШЛЫГЫ

РАСПОРЯЖЕНИЕ БОЕРЫК

28.10.2024 с. Верхний Услон 41

О назначении ответственного лица за обеспечение информационной безопасности в Совете Верхнеуслонского муниципального района

В целях выполнения требований Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»:

1. Назначить заместителя главы Верхнеуслонского муниципального района Осянина Сергея Викторовича ответственным за:

- обеспечение информационной безопасности в Совете Верхнеуслонского муниципального района;
- обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

2. Утвердить положение об ответственном лице за обеспечение информационной безопасности в Совете Верхнеуслонского муниципального района (Приложение №1).

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава Верхнеуслонского муниципального района **Е.А.Варакин**

РЕСПУБЛИКА ТАТАРСТАН Р.06-157/02 Совет Верхнеуслонского муниципального района ИНН 1615005848 Югары Ослан муниципаль районы Советы ТАТАРСТАН РЕСПУБЛИКАСЫ

Приложение №1
к Распоряжению главы
Верхнеуслонского
муниципального района
от «____» _____2024 г. №___

Положение об ответственном лице за обеспечение информационной безопасности в Совете Верхнеуслонского муниципального района

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об ответственном лице за обеспечение информационной безопасности в Совете Верхнеуслонского муниципального района (далее - Ответственное лицо) определяет полномочия, права, обязанности и ответственность сотрудника, на которого возложена ответственность за:

- обеспечение информационной безопасности в Совете Верхнеуслонского муниципального района;
- обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерных инциденты.

1.2. Ответственное лицо назначается Главой Верхнеуслонского муниципального района из числа его заместителей.

1.3. Ответственное лицо подчиняется непосредственно Главе Верхнеуслонского муниципального района.

1.4. Указания и поручения Ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми сотрудниками Совета Верхнеуслонского муниципального района (далее - Совет).

2. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ

2.1. Ответственное лицо должно назначаться из числа заместителей Главы Верхнеуслонского муниципального района, имеющих высшее образование.

2.2. Ответственное лицо должно обладать следующими знаниями, умениями, профессиональными компетенциями:

Основные (в том числе производственные, бизнес н управленческие) процессы Совета и специфика обеспечения безопасности Совета.

Влияние информационных технологий на деятельность Совета, в том числе:

- роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования;
- зависимость основных процессов функционирования.

Информационно телекоммуникационные технологии, в том числе:

- современные информационно-телекоммуникационные технологии, используемые в Совете;
- способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа;
- типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;
- принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей.

Обеспечение информационной безопасности, в том числе:

- цели, задачи, основы организации, ключевые элементы, основные способы н средства обеспечения информационной безопасности;
- цели обеспечения информационной безопасности применительно к основным процессам функционирования Совета, реализация и контроль их достижения;
- принципы и направления стратегического развития информационной безопасности в Совете;
- правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Совете, состав и содержание таких документов;
- порядок организации работ по обеспечению информационной безопасности в Совете;
- основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности Совета для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности Совета;
- основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;
- возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;
- способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;
- порядок организации взаимодействия структурных подразделений Совета при решении вопросов обеспечения информационной безопасности;

- управление проектами по информационной безопасности;
- антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;
- планирование деятельности по обеспечению информационной безопасности в Совете;
- формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Совета;
- организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в Совете;
- внедрение политики;
- организация контроля и анализа применения политики;
- организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в Совете;
- поддержка и совершенствование деятельности по обеспечению информационной безопасности в Совете;
- организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в Совете;
- организация внедрения способов и средств для обеспечения информационной безопасности в Совете;
- организация мероприятий по анализу и контролю состояния информационной безопасности Совета и модернизации (трансформации) процессов функционирования Совета в целях обеспечения информационной безопасности в Совете;
- обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;
- организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Совета и реагированию на компьютерные инциденты;
- организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в Совете.

2.3. С учетом области и вида деятельности Совета от Ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

– защиты государственной тайны:

– защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;

– обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

– обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

– создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;

– создания, обеспечения технических условий установки и эксплуатации средств защиты информации;

– иных нормативных правовых актов и стандартов в области информационной безопасности.

3. ТРУДОВЫЕ (ДОЛЖНОСТНЫЕ) ОБЯЗАННОСТИ

3.1. Ответственное лицо принимает участие в формировании политики Совета, отвечает за согласование стратегии развития Совета в части вопросов обеспечения информационной безопасности.

3.2. Ответственное лицо:

– Организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности Совета и его (ее) процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в Совете, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики.

– Организует работу по обеспечению информационной безопасности Совета, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену.

– Организует реализацию и контроль проведения в Совете организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно Ответственным лицом в результате своей деятельности.

– Организует беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам,

принадлежащим ведомству либо используемым Советом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга их защищенности, а также сотрудникам структурного подразделения, осуществляющего функции по обеспечению информационной безопасности.

– Организует взаимодействие с должностными лицами Федеральной службы безопасности Российской Федерации и ее территориальных органов, в том числе контроль исполнения указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих ведомству либо используемых Советом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет».

– Организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся зашиты информации.

– Организует развитие информационной безопасности, формирование и развитие навыков сотрудников Совета в сфере информационной безопасности.

– Организует разработку и реализацию мероприятий по обеспечению информационной безопасности в Совете в соответствии с требованиями по обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

– Организует контроль пользователей информационных ресурсов Совета в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации.

– Организует планирование мероприятий по обеспечению информационной безопасности в Совете.

– Организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Совете, осуществляет согласование иных документов Совета в части обеспечения информационной безопасности.

– Организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в Совете.

– Организует проведение контроля за состоянием обеспечения информационной безопасности в Совете, включая оценку защищенности систем и сетей, оператором которых является.

3.3. Ответственное лицо:

– Осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в Совете, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в Совете, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак.

– Осуществляет регулярное и своевременное информирование руководства Совета о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в Совете и результатах практических учений по противодействию компьютерным атакам.

– Осуществляет контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы.

– Осуществляет согласование требований к системам и сетям, оператором которых является Совет, в части обеспечения информационной безопасности.

3.4. Ответственное лицо:

– Организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности Совета и контролирует их результаты.

– Организует и контролирует функционирование системы обеспечения информационной безопасности в Совете.

3.5. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации Совета.

3.6. Ответственное лицо с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами ведомств, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

– Силами структурного подразделения, ответственного за обеспечение информационной безопасности, с заключением соглашения (издания совместного акта) о взаимодействии с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по

компьютерным инцидентам), включающего в том числе права и обязанности сторон, порядок проведения совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля.

– Силами структурного подразделения, ответственного за обеспечение информационной безопасности, с его аккредитацией как центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

– Силами организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3.7. Ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства зашиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

3.8. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

3.9. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Совете.

3.10. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в Совете.

3.11. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

3.12. Ответственное лицо выполняет иные обязанности, исходя из возложенной ответственности и поставленных руководством Совета задач в рамках обеспечения информационной безопасности Совета.

3.13. Ответственное лицо:

– Соблюдает и обеспечивает выполнение законодательства Российской Федерации.

– В случаях, установленных законодательством Российской Федерации, согласовывает политику с Федеральной службой безопасности Российской

Федерации и Федеральной службой по техническому и экспортному контролю.

– Представляет по запросам Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в Совете.

– Поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в Совете.

– Организовывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, семинарах, конференциях, работе межведомственных рабочих группах, отраслевых экспертных сообществ, международных органов н организаций.

– Участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

4. ПРАВА ОТВЕТСТВЕННОГО ЛИЦА

4.1. Ответственное лицо имеет право:

– Давать указания и поручения сотрудникам Совета в части обеспечения информационно безопасности.

– Запрашивать от сотрудников Совета информацию и материалы, необходимые для реализации возложенных на Ответственное лицо прав и обязанностей.

– Участвовать в заседаниях (совещаниях) коллегиальных органов Совета, принятии решений по вопросам деятельности Совета, а также по внесению предложений по совершенствованию деятельности Совета.

– Участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу Совета.

– Представлять результаты реализации политики коллегиальному органу Совета.

– Принимать решения по вопросам обеспечения информационной безопасности Совета.

– Взаимодействовать с Федеральной службой безопасности Российской Федерации. Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности.

– Вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности.

– Инициировать проверки уровня (состояния) обеспечения информационной безопасности в Совете.

– Организовывать на объектах Совета мероприятия по информационной безопасности, разрабатывать и представлять Главе Верхнеуслонского муниципального района предложения по внесению изменений в процессы функционирования, принимать другие меры, направленные на недопущение реализации негативных последствий.

– Получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации.

– Обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей Ответственного лица.

5. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЛИЦА

5.1. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность:

– За неисполнение или ненадлежащее исполнение своих обязанностей.

– За действия (бездействие), ведущие к нарушению прав и законных интересов Совета.

– За разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей.

– За достижение целей обеспечения информационной безопасности.

– За поддержание н непрерывное развитие информационной безопасности Совета для исключения (невозможности реализации) негативных последствий.

– За организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности Совета.

– За нарушения требований по обеспечению информационной безопасности.

– За нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.