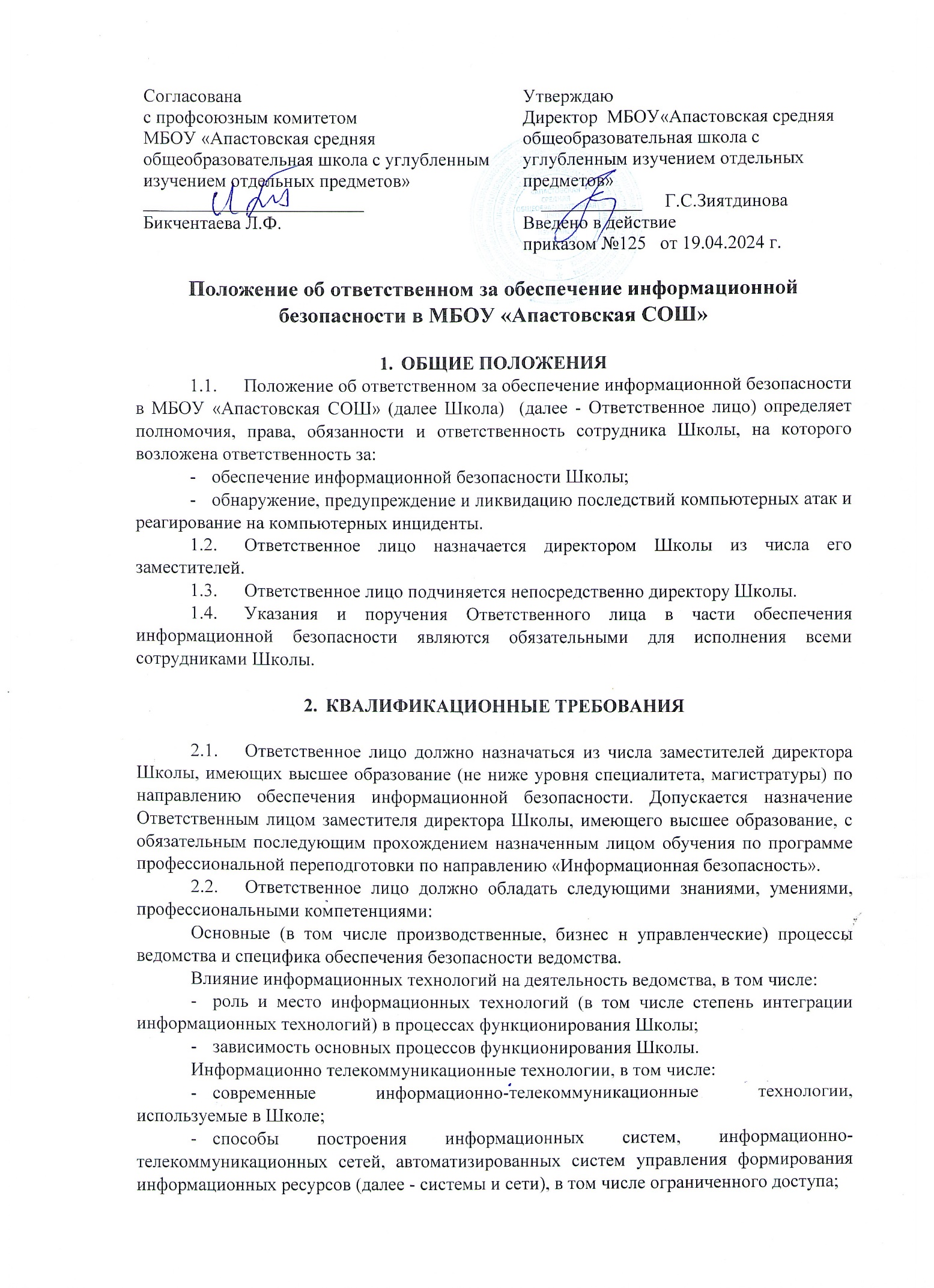
****

- 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 и средства обеспечения информационной безопасности;

- цели обеспечения информационной безопасности применительно к основным процессам функционирования Школы, реализация и контроль их достижения;

- принципы и направления стратегического развития информационной безопасности в Школе;

- правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Школе, состав и содержание таких документов;

- порядок организации работ по обеспечению информационной безопасности в Школе;

- основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности Школы для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности Школы;

- 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 Школы 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 Школе;

- формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Школы;

- организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в Школе;

- внедрение политики;

- организация контроля и анализа применения политики;

- организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в Школе;

- поддержка и совершенствование деятельности по обеспечению информационной безопасности в Школе;

- организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в Школе;

- организация внедрения способов и средств для обеспечения информационной безопасности в Школе;

- организация мероприятий по анализу и контролю состояния информационной безопасности Школы и модернизации (трансформации) процессов функционирования Школы в целях обеспечения информационной безопасности в Школе;

- 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 Школы и реагированию на компьютерные инциденты;

- организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в Школе.

2.3. С учетом области и вида деятельности Школы 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 Школы, отвечает за согласование стратегии развития Школы в части вопросов обеспечения информационной безопасности.

3.2. Ответственное лицо:

* Организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности Школы и его (ее) процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в Школе, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики.
* Организует работу по обеспечению информационной безопасности Школы, 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 Школе 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 Школе либо используемым Школой, 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 Школе либо используемых Школой, 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 Школы в сфере информационной безопасности.
* Организует разработку и реализацию мероприятий по обеспечению информационной безопасности в Школе 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 ведомства 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 Школе.
* Организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Школе, осуществляет согласование иных документов Школы в части обеспечения информационной безопасности.
* Организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в Школе.
* Организует проведение контроля за состоянием обеспечения информационной безопасности в Школе, включая оценку защищенности систем и сетей, оператором которых является Школа.

3.3. Ответственное лицо:

* Осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в Школе, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в Школе, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак.
* Осуществляет регулярное и своевременное информирование руководства Школы о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в Школе 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 Школа, в части обеспечения информационной безопасности.
* Осуществляет руководство структурным подразделением Школа, обеспечивающим информационную безопасность Школы.

3.4. Ответственное лицо:

* Организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности Школы и контролирует их результаты.
* Организует и контролирует функционирование системы обеспечения информационной безопасности в Школе.
* Координирует деятельность иных структурных подразделений Школы по вопросам обеспечения информационной безопасности.

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

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 Школы, 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 Школе.

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

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 школы задач в рамках обеспечения информационной безопасности Школы.

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 Школе.
* Поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в Школе.
* Организовывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, 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 Школы в части обеспечения информационно безопасности.
* Запрашивать от сотрудников Школы информацию и материалы, необходимые для реализации возложенных на Ответственное лицо прав и обязанностей.
* Участвовать в заседаниях (совещаниях) коллегиальных органов Школы, принятии решений по вопросам деятельности Школы, а также по внесению предложений по совершенствованию деятельности Школы.
* Участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу Школы.
* Представлять результаты реализации политики коллегиальному органу Школы.
* Принимать решения по вопросам обеспечения информационной безопасности Школы.
* 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 Школе ее подведомственных и дочерних организациях (при наличии таковых).
* Организовывать на объектах Школы мероприятия по информационной безопасности, разрабатывать и представлять руководителю ведомства 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 Школы.
* 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 Школы для исключения (невозможности реализации) негативных последствий.
* За организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности Школы.
* За нарушения требований по обеспечению информационной безопасности.
* За нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.