



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ
(РОСТЕХНАДЗОР)**

П Р И К А З

30 января 2023г.

Москва

№ 20

**Об утверждении Концепции
формирования и развития культуры информационной безопасности
работников Федеральной службы по экологическому,
технологическому и атомному надзору**

В целях формирования и развития культуры информационной безопасности работников Федеральной службы по экологическому, технологическому и атомному надзору в соответствии с Концепцией формирования и развития культуры информационной безопасности граждан Российской Федерации, утвержденной распоряжением Правительства Российской Федерации от 22 декабря 2022 г. № 4088-р, приказываю:

1. Утвердить Концепцию формирования и развития культуры информационной безопасности работников Федеральной службы по экологическому, технологическому и атомному надзору (далее – Концепция) согласно приложению к настоящему приказу.

2. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель

А.В. Трембицкий

Приложение
к приказу Федеральной службы
по экологическому, технологическому
и атомному надзору
от «30» января 2023 г. № 20

КОНЦЕПЦИЯ

формирования и развития культуры информационной безопасности
работников Федеральной службы по экологическому,
технологическому и атомному надзору

I. Общие положения

Стремительное развитие информационных технологий поспособствовало реализации одного из важнейших прав – права на свободу и доступ к информации, но при этом значительно увеличило количество угроз информационной безопасности как для отдельного гражданина Российской Федерации, так и для государства в целом.

Угрозы информационной безопасности с технической точки зрения подразумевают под собой утечку информации, несанкционированный доступ к информационным ресурсам, нарушение функционирования (работоспособности) информационных систем или их компонентов, несанкционированный массовый сбор информации и другие. С психологической точки зрения к угрозам информационной безопасности можно отнести травлю в цифровом пространстве, пропаганду насилия, национализма, распространение недостоверной информации и другой вредоносный контент.

Указанные угрозы информационной безопасности оказывают деструктивное влияние на все сферы жизни граждан Российской Федерации - профессиональную, материальную, морально-психологическую, а следовательно, отрицательно сказываются и на государстве в целом. При этом эффективно противостоять указанным угрозам достаточно проблематично, поскольку жизнь современного человека неразрывно связана с пребыванием в информационном пространстве.

В этой связи особую актуальность принимает вопрос формирования и развития культуры информационной безопасности.

Культура информационной безопасности - это совокупность сформированных знаний, умений и навыков по вопросам информационной безопасности, обеспечивающая безопасное пребывание гражданина Российской Федерации в информационном пространстве.

Культура информационной безопасности затрагивает и профессиональную, и бытовую деятельность граждан Российской Федерации, причем в профессиональной деятельности культура

информационной безопасности неразрывно связана с вопросами корпоративной информационной безопасности, в бытовой – с личной информационной безопасностью.

При этом, рассматривая вопрос корпоративной информационной безопасности, особое значение, в том числе ввиду текущей геополитической обстановки, имеет вопрос соблюдения правил информационной безопасности в органах государственной власти при осуществлении лицами, замещающими должности государственной гражданской и муниципальной службы, своих должностных обязанностей.

В этой связи необходимо прививать работникам Ростехнадзора вне зависимости от возраста или сферы деятельности знания по всему спектру вопросов информационной безопасности, таких как распознавание фишинговых сайтов и писем, телефонного мошенничества, создание надежных паролей, распознавание недостоверной информации и другого вредоносного контента.

Такой подход будет способствовать непосредственному повышению общего уровня грамотности работников Ростехнадзора по вопросам информационной безопасности, сокращению финансового, морально-психологического и репутационного ущерба от преступлений с использованием информационно-коммуникационных технологий, сохранности данных работников Ростехнадзора, в том числе персональных, повышению уровня доверия к цифровым сервисам, а также дальнейшей цифровизации экономики Российской Федерации.

II. Основные принципы повышения уровня культуры информационной безопасности работников Ростехнадзора

Исходя из необходимости и важности общего повышения грамотности по вопросам информационной безопасности работников Ростехнадзора и с учетом формирования практических и психологических навыков, мероприятия по развитию культуры информационной безопасности работников Ростехнадзора реализуются в соответствии со следующими принципами:

ответственность государства за соблюдение законных интересов граждан Российской Федерации в информационной сфере;

консолидация усилий структурных подразделений Ростехнадзора в работе по повышению грамотности работников Ростехнадзора в вопросах информационной безопасности;

осуществление Ростехнадзором работ по совершенствованию законодательства Российской Федерации, позволяющего на регулярной основе осуществлять реализацию мероприятий по повышению грамотности по вопросам информационной безопасности лиц, замещающих должности государственной гражданской службы Российской Федерации;

проведение адаптированной информационной кампании для работников Ростехнадзора как основного способа повышения культуры информационной безопасности;

проведение на регулярной основе иных мероприятий, направленных на повышение грамотности работников Ростехнадзора по вопросам информационной безопасности;

формирование у работников Ростехнадзора ответственного отношения к информационной безопасности в цифровом пространстве.

III. Приоритетные задачи в области повышения уровня культуры информационной безопасности работников Ростехнадзора

Целью реализуемых мероприятий по повышению культуры информационной безопасности работников Ростехнадзора является формирование у них навыков противодействия угрозам информационной безопасности, в том числе информационно-психологическим угрозам, и, как следствие, повышение общего уровня грамотности по вопросам информационной безопасности.

Для достижения указанной цели необходимо обеспечить решение следующих задач:

обучение работников Ростехнадзора новым образцам поведения, основанным на правилах информационной безопасности;

выработка мероприятий по регулярному повышению грамотности по вопросам информационной безопасности лиц, замещающих должности государственной гражданской службы Российской Федерации;

донесение на регулярной основе до работников Ростехнадзора значимости проблемы и последствий несоблюдения правил информационной безопасности;

формирование у работников Ростехнадзора, не интересующихся вопросами информационной безопасности, интереса к указанной теме;

проведение на регулярной основе мониторинга уровня грамотности работников Ростехнадзора по вопросам информационной безопасности, в том числе путем проведения ежегодного тестирования;

повышение доверия к цифровым сервисам, в том числе к государственным;

снижение актуальности угроз информационной безопасности, а также повышение эффективности противодействия их реализации;

выстраивание взаимодействия Ростехнадзора с органами государственной власти, неправительственными и коммерческими организациями, направленного на повышение грамотности работников Ростехнадзора по вопросам информационной безопасности;

создание дополнительных точек взаимодействия с работниками Ростехнадзора в целях эффективного донесения до них информации о важности соблюдения правил информационной безопасности.

IV. Механизмы реализации повышения уровня культуры информационной безопасности работников Ростехнадзора

В рамках повышения культуры информационной безопасности работников Ростехнадзора необходима выработка комплексного подхода, подразумевающего ряд мероприятий, среди которых:

проведение общей информационной кампании для работников Ростехнадзора, направленной на повышение грамотности по вопросам информационной безопасности. Информационная кампания по вопросам информационной безопасности должна охватывать не только тех работников Ростехнадзора, кто уже вовлечен в тему информационной безопасности и обладает определенными знаниями в этой области, но и работников Ростехнадзора, которые самостоятельно не интересуются указанными вопросами. Указанная информационная кампания должна актуализироваться на ежегодной основе, а при ее проведении должен применяться весь спектр средств продвижения, включая информационные ресурсы и интерактивное общение с пользователями. Вместе с тем целесообразным является разработка учебно-методических материалов, а также специальных курсов по информационной безопасности, содержащих информацию об актуальных вопросах информационной безопасности;

повышение грамотности по вопросам информационной безопасности лиц, замещающих должности государственной гражданской службы Российской Федерации. Учитывая специфику прохождения гражданской службы, при повышении грамотности работников Ростехнадзора принципиально важным является параллельное освоение теоретических и практических навыков по вопросам информационной безопасности. Стремительное увеличение угроз информационной безопасности, обусловленное в том числе складывающейся геополитической обстановкой, требует быстрого получения первых положительных результатов от реализации мероприятий, направленных на повышение грамотности по вопросам информационной безопасности. При этом важно, чтобы лицо, проходящее государственную гражданскую службу Российской Федерации, получало не только теоретические навыки по вопросам информационной безопасности, но и умело противостоять угрозам информационной безопасности в реальной жизни. Соответственно в повышении грамотности гражданских служащих по вопросам информационной безопасности важен баланс теории и практики. При этом важно отметить, что мероприятия по повышению грамотности лиц, замещающих должности государственной гражданской службы Российской Федерации, должны осуществляться на регулярной основе. В этой связи, в том числе ввиду специфики осуществления служебной деятельности, предполагающей наличие навыков безопасного использования информационных технологий, отсутствие которых может нанести ущерб объектам информационной инфраструктуры

Ростехнадзора, должна быть предусмотрена обязанность лиц, замещающих должности государственной гражданской службы Российской Федерации, участвовать на ежегодной основе в мероприятиях, направленных на повышение грамотности по вопросам информационной безопасности.

V. Ожидаемые результаты

Реализация настоящей концепции должна способствовать повышению уровня грамотности работников Ростехнадзора по вопросам информационной безопасности, сокращению финансового, морально-психологического и репутационного ущерба от преступлений с использованием информационно-коммуникационных технологий, сохранности данных работников Ростехнадзора, в том числе персональных, повышению уровня доверия к цифровым сервисам, а также дальнейшей цифровизации экономики Российской Федерации.