Приложение № 13

к приказу наименование организации

от « » №

**Инструкция пользователя государственной информационной системы «АЦК-Госзаказ» по работе со служебной электронной почтой и сторонними веб-ресурсами**

**Правила использования служебной электронной почты**

1. Электронная почта предоставляется работникам компании только для исполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

2. Электронная почта используется для обмена служебной информацией
в виде текстовых сообщений или электронных документов.

3. Пользователям ЗАПРЕЩАЕТСЯ:

3.1. использовать служебную электронную почту в личных целях;

3.2. производить рассылку любых материалов, не связанных
с исполнением должностных обязанностей;

3.3. пересылать исполняемые файлы (с расширениями – .exe, .dll, .pif
и т.п.);

3.4. пересылать мультимедийные файлы (аудио и видео);

3.5. производить рассылку вредоносных программ или файлов, зараженных вирусами;

3.6. использовать электронную почту для передачи материалов большого объема (суммарный объём пересылаемой информации – не более 10 Мб);

3.7. предоставлять кому бы-то ни было пароль доступа к своему почтовому ящику;

3.8. пересылать по электронной почте пароли, реквизиты доступа
к служебным ресурсам;

3.9. отправлять кому-либо информацию ограниченного доступа. Пересылка по электронной почте информации ограниченного доступа (в том числе персональных данных, служебных документов и т.д.) допускается только по согласованию с подразделением, на которое возложены функции
по обеспечению информационной безопасности. При пересылке такой информации обязательно использование средств криптографической защиты информации в соответствии с указаниями сотрудника подразделения,
на которое возложены функции по обеспечению информационной безопасности;

3.10. открывать письма с названием темы типа «наследство», «выигрыш
в лотерею» («африканские» письма) и т.п.;

3.11. открывать вложения, представляющие собой исполняемые файлы, либо имеющие неизвестные Вам расширения, независимо от адреса отправителя;

3.12. открывать вложения без антивирусной проверки файла;

3.13. вводить «защитные коды» и пароли на высланные ресурсы без предварительной договорённости с отправителем;

3.14. открывать файлы, не предназначенные Вам (никогда не открывайте файлы, которые попали к Вам по ошибке — например, не открывайте присланное Вам резюме, если Вы не работаете в отделе кадров — перешлите письмо им или не отвечайте вовсе);

3.15. включать использование макросов, «активного содержимого», скрипты и ActiveX в Microsoft Office;

3.16. помогать открывать «не открывающиеся» файлы. При проблемах
с открытием вложений следует обратиться в подразделение, на которое возложены функции по обеспечению информационной безопасности;

3.17. использовать на рабочем месте личную (неслужебную) электронную почту.

**Правила работы с веб-ресурсами.**

1. При работе с веб-ресурсами Пользователям ЗАПРЕЩАЕТСЯ:
* сохранять аутентификационную информацию с помощью браузера (галочка «запомнить меня», кнопка «сохранить пароль» и подобные);
* скачивать и запускать любые исполняемые файлы без согласования с подразделением, на которое возложены функции по обеспечению информационной безопасности;
* отключать во время работы средства антивирусной защиты или добавлять в исключения антивируса файлы без согласования с подразделением, на которое возложены функции по обеспечению информационной безопасности.
1. При работе с веб-ресурсами Пользователям РЕКОМЕНДУЕТСЯ:
* убедиться, что адрес сайта (URL) в адресной строке браузера набран корректно;
* убедиться, что URL является безопасным и начинается с «https:\\»;
* обратить внимание на любые расхождения с тем, как обычно выглядит интересующая вас веб-страница.
1. При наличии сомнений в корректности работы используемого веб-ресурса или его подлинности необходимо обратиться в подразделение,
на которое возложены функции по обеспечению информационной безопасности.