УТВЕРЖДЕНО
Решением Председателя правления
АО «Институт развития
Электроэнергетики и энергосбережения
(Казахэнергоэкспертиза)»
«16» _____ 2024 г.

Правила использования сети Интернет и электронной почты

Астана, 2024 г.

Оглавление

1. Общие положения и основные понятие 3
2. Управление доступом 3
3. Обеспечение информационной безопасности 3
4. Обязанности работника 4
5. Проведение проверок и ответственность 5
6. Ответственность 6
Приложение 1 7

1. ОБЩИЕ ПОЛОЖЕНИЯ И ОСНОВНЫЕ ПОНЯТИЕ

1. Настоящие Правила использования сети Интернет и электронной почты (далее - Правила), регламентирует предоставление и ограничение доступа, а также работу с электронной почтой и в сети Интернет
2. В Правилах используются следующие основные термины и определения:

Общество – АО "Институт развития электроэнергетики и энергосбережения" ("Казахэнергоэкспертиза");

Служба технической поддержки Общества (далее – **Служба)** – подразделение(я), ответственное(ые) за администрирование, сопровождение и обеспечение бесперебойного функционирования Системы;

Структурное подразделение информационной безопасности – структурное подразделение, ответственное за обеспечение информационной безопасности.

Администратор – работник, представляющий услуги системного администрирования и технической поддержки;

ИТ – информационные технологии;

Сотрудник по информационной безопасности (далее – Сотрудник по ИБ) – лицо, назначенное ответственным руководством Общества за управление мероприятиями в области информационной безопасности. Сотрудник по информационной безопасности может быть назначен для осуществления только данной деятельности или совмещать ее с функциями создания, изменения, удаления права доступа и ролей Пользователей;

Локальная сеть внешнего контура (далее – ЛС внешнего контура) – локальная сеть Общества, отнесенная к внешнему контуру телекоммуникационной сети Общества, имеющая соединение с Интернетом, доступ к которому для Общества предоставляется операторами связи только через единый шлюз доступа к Интернету.

2. УПРАВЛЕНИЕ ДОСТУПОМ

3. Всем сотрудникам Общества предоставляется доступ к корпоративной почтовой службе и доступ к сети Интернет, по средствам их персональных компьютеров.

3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4. Должен быть установлен максимальный размер прикрепляемых файлов, а также максимальный размер электронного ящика;

5. Руководство или сотрудник по ИБ Общества вправе определить типы файлов, запрещенные к отправке и получению посредством электронной почты, а также запрещённые скачивать из сети Интернет.
6. Подключение к сети Интернет осуществляется через ЛС внешнего контура.
7. Доступ к сети интернет предоставляется с использованием корпоративного прокси сервера.
8. Настройка компьютеров производится Администратором службы технической поддержки Общества.
9. Доступ к ресурсам сети Интернет может быть ограничен по решению руководства или сотрудника по ИБ Общества. Сотрудник по ИБ разрабатывает и по мере необходимости актуализирует список запрещенных ресурсов и веб-сайтов доступных в сети Интернет (Приложение 1).
10. Администраторы устанавливают фильтры нежелательных данных, ресурсов, контента и т.д. с помощью инструментов ИТ.
11. Все события серверов электронной почты и прокси подлежат регистрации в системном журнале.
12. Все электронные письма должны просматриваться в журналах регистрации Сотрудником по ИБ. В случае выявления нарушений, права доступа пользователя могут быть ограничены и (или) на пользователя может быть наложено дисциплинарное взыскание;

4. ОБЯЗАННОСТИ РАБОТНИКА

13. Сотрудники Общества во время работы с почтовой службой или в сети Интернет должны соблюдать требования документа «Правила идентификации, классификации и маркировки активов, связанные со средствами обработки информации»
14. Соблюдать общепринятые нормы и правила обмена почтовыми сообщениями.
15. Использовать почтовую службу и Интернет для решение служебных задач.
16. Решение иных задач кроме служебных, осуществлять в нерабочее время, за исключением случаев, когда существует вероятность угрозы здоровью или жизни человека.
17. Сотрудникам Общества запрещается:
    - использование ресурсов Интернета для хранения служебной информации;
    - использование ресурсов Интернета и электронной почты в неслужебных целях;
    - копирование из Интернета любых программ, архивов и данных, не имеющих прямого отношения к служебным обязанностям сотрудника;

- пересылка по электронной почте Интернета служебной информации, содержащей государственную тайну, в незашифрованном виде;
- доступ к сети Интернет и электронной почте не со своего рабочего места с использованием данных своей учетной записи.
- предоставление доступа к сети Интернет с использованием данных своей учетной записи другим лицам.
- публикация своего адреса электронной почты в электронных каталогах и на поисковых машинах сети Интернет.
- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.п., не связанные с выполнением пользователем функциональных обязанностей.
- открытие (запуск на выполнение) файла, полученного из сети Интернет или по электронной почте, без предварительной проверки его антивирусным программным обеспечением.
- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.
- использовать анонимные прокси серверы.

5. ПРОВЕДЕНИЕ ПРОВЕРОК И ОТВЕТСТВЕННОСТЬ

18. При попытке получения доступа к запрещенному контенту пользователем, администратор делает предупреждение о необходимости прекратить данные действия. В крайних случаях, после нескольких предупреждений доступ к сети Интернет может быть временно закрыт, и на пользователя может быть наложено дисциплинарное взыскание, в зависимости от степени тяжести нарушения;
19. Использование сети Интернет сотрудниками Общества может отслеживаться и регистрироваться, данные регистрации могут использоваться в качестве доказательств в случае принятия дисциплинарных мер.
20. Служба технической поддержки Общества проводит анализ инцидентов информационной безопасности по фактам нарушений требований защиты информации при работе с электронной почтой и Интернет совместно с структурным подразделением информационной безопасности.
21. В случае обнаружения фактов или выявления потенциальной угрозы информационной безопасности Администратор немедленно информирует Сотрудника по ИБ.

6. ОТВЕТСТВЕННОСТЬ

22. Сотрудники Общества несут персональную ответственность за надлежащее выполнение Правил, в рамках законодательства Республики Казахстан и внутренних нормативных документов Общества.
23. Контроль исполнения настоящих правил осуществляет Специалист по ИБ.

ПРИЛОЖЕНИЕ 1

к Правилам использования сети
Интернет и электронной почты

Запрещенные ресурсы и веб-сайты сети Интернет доступ к которым необходимо ограничить

Перечень категорий Интернет-ресурсов

№ п.п.	Название категории (на английском языке)	Название категории (на русском языке)	Описание категории

Перечень веб-сайтов

№ п.п.	URL	Название веб-сайта	Описание