**Инструкция по обеспечению информационной безопасности интернет-ресурсов**

**Общие положения**

Рекомендации по обеспечению информационной безопасности (далее – безопасность) интернет-ресурсов (далее – ресурсы) разработаны в целях унификации подходов к обеспечению безопасности ресурсов Федерации профсоюзов Беларуси и ее членских организаций.

Рекомендации должны быть использованы в работе специалистами по информационной работе, на которых официально возложены функции администрирования и сопровождения ресурсов и которые несут персональную ответственность за обеспечение информационной безопасности ресурсов.

Виды основных угроз безопасности ресурсов:

- нежелательный контент;

- несанкционированный доступ;

- потеря данных;

- мошенничество.

К мероприятиям обеспечения информационной безопасности относятся:

определение круга ответственных лиц, имеющих доступ к администрированию ресурсов, определение их обязанностей и ответственности;

обеспечение регулярной смены доступов к администрированию ресурсов, в том числе в случае смены лиц, ответственных за их администрирование;

выполнение инструкции (методических рекомендаций) в случае выявления фактов размещения на информационном ресурсе несанкционированной (дискредитирующей) информации;

выполнение инструкции (методических рекомендаций) в случае выявления технических неисправностей и сбоев в работе информационных ресурсов.

**Организация обеспечения безопасности ресурсов**

1. Определение круга лиц, допущенных к администрированию ресурсов.

Круг лиц, допущенных к администрированию ресурсов, определяется руководителями областных, районных, городских объединений профсоюзов, членских организаций ФПБ и их областных (городских), районных, объединенных отраслевых организаций, а также Унитарного предприятия «Издательский Дом «Проф-Пресс» (далее – руководитель организации).

Количество лиц, допущенных к администрированию ресурсов, определяется реальной необходимостью обеспечения функционирования ресурса и исходя из минимально необходимого для этого количества персонала.

1. Доступ к администрированию ресурса осуществляется только с использованием персонифицированного и уникального имени пользователя (логина) и пароля.

Генерацию и персонализированную (под роспись) выдачу логина и пароля руководителям организаций осуществляет Унитарное предприятие «Издательский Дом «Проф-Пресс» (далее – УП «ИД «Проф-Пресс»), за исключением тех организаций, у которых не заключен договор на техническое сопровождение их ресурсов с УП «ИД «Проф-Пресс».

Персонифицированную (под роспись) выдачу логинов и паролей лицам, допущенным к администрированию ресурсов, осуществляет руководитель организации.

При необходимости предоставления временного доступа лицу, временно замещающему специалиста, допущенного к администрированию ресурсов, руководитель организации обращается в УП «ИД «Проф-Пресс» для предоставления временных логина и пароля с обоснованием необходимости и сроков их действия, за исключением руководителей тех организаций, у которых не заключен договор на техническое сопровождение их ресурсов с УП «ИД «Проф-Пресс».

В случае смены сотрудника, допущенного к администрированию ресурса, руководитель организации обращается в УП «ИД «Проф-Пресс» для произведения блокировки действующих логина и пароля и в случае необходимости предоставления новых, за исключением руководителей тех организаций, у которых не заключен договор на техническое сопровождение их ресурсов с УП «ИД «Проф-Пресс».

Смена логинов и паролей производится силами УП «ИД «Проф-Пресс» не реже одного раза в квартал на регулярной основе и немедленно в случае возникновения предпосылок или признаков их компрометации.

Передача персонифицированных логинов и паролей иным лицам запрещена.

Руководителей тех организаций, у которых не заключен договор на техническое сопровождение их ресурсов с УП «ИД «Проф-Пресс», самостоятельно реализуют мероприятия по обеспечению безопасного доступа сотрудников к администрированию ресурса, руководствуясь положениями настоящей инструкции, и несут за это персональную ответственность.

1. В случае выявления факта размещения на ресурсе несанкционированной (дискредитирующей) информации лицо, допущенное к администрированию ресурса, сообщает об этом руководителю организации, информирует пресс-службу ФПБ и предпринимает меры к скрытию из открытого доступа выявленной информации. Для чего с использованием программных средств администрирования (консоли управления ресурсом) снимает указанную информацию с публикации, не удаляя ее, и сообщает об этом организации, осуществляющей техническое сопровождение ресурса. В дальнейшем выполняет указания руководителя организации и рекомендации организации, осуществляющей техническое сопровождение ресурса.
2. В случае выявления технических неисправностей и сбоев в работе ресурса лицо, допущенное к его администрированию, сообщает об этом руководителю организации, информирует пресс-службу ФПБ, а также организацию, осуществляющую техническое сопровождение ресурса. В дальнейшем выполняет указания руководителя организации и рекомендации организации, осуществляющей техническое сопровождение ресурса.

**Порядок работы в сети Интернет**

1. Не сохранять данные для входа в аккаунт (логин и пароль) в браузере.
2. Не использовать открытые и общественные сети Wi-Fi для подключения к сети Интернет.
3. Обеспечить наличие доверенного антивирусного программного обеспечения на всех связанных с аккаунтом устройствах.
4. Завершая работу по администрированию сайта, выходить из панели администрирования (завершать сеанс).
5. Не открывать подозрительные письма, не открывать и не запускать файлы, вложенные в письмо, если отправитель вам не известен.
6. Не переходить по подозрительным ссылкам, полученным в письмах, мессенджерах, а также в соцсетях, если отправитель вам не известен.