ИНСТРУКЦИЯ ПО НАСТРОЙКАМ И ИСПОЛЬЗОВАНИЮ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЕБ-СИСТЕМЕ WWW.UFS-ONLINE.RU

СОДЕРЖАНИЕ

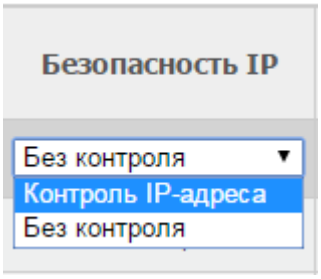
1. НАЗНАЧЕНИЕ

Соблюдение всех требований и рекомендаций по Информационной безопасности, а также использование всех функций информационной безопасности Веб-системы www.ufs-online.ru, помогут предотвратить несанкционированное оформление железнодорожных билетов за Ваш счет, с последующей сдачей их в кассах РЖД.

2. ВКЛЮЧЕНИЕ ПРИВЯЗКИ ПО IP.

В Веб-системе www.ufs-online.ru есть возможность задать перечень IP адресов, с которых возможен вход под учетной записью.

Данная функция включается в Интерфейсе Администратора на вкладке «Сотрудники». Для каждого сотрудника можно включить и выключить эту функцию.



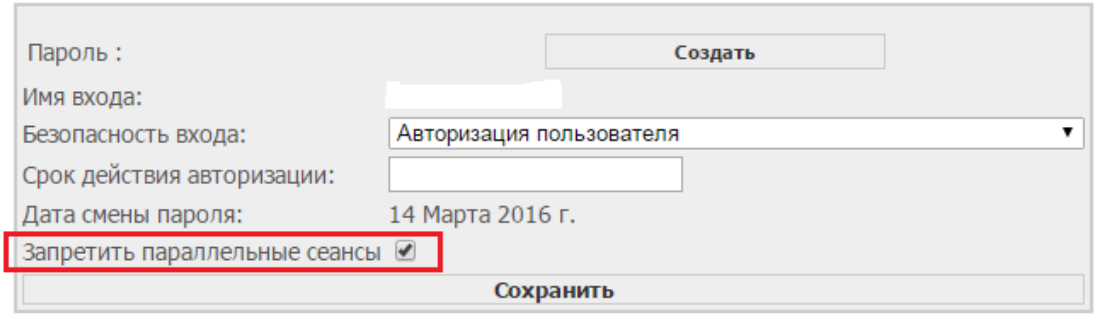
Включение контроля IP-адреса не позволяет злоумышленнику воспользоваться вашей учетной записью с другого ПК, даже если ему известен пароль.

IP-адрес Агента/Партнера указывается в договоре в Разделе 8 «Юридические адреса и банковские реквизиты сторон» в поле «IP – адрес».

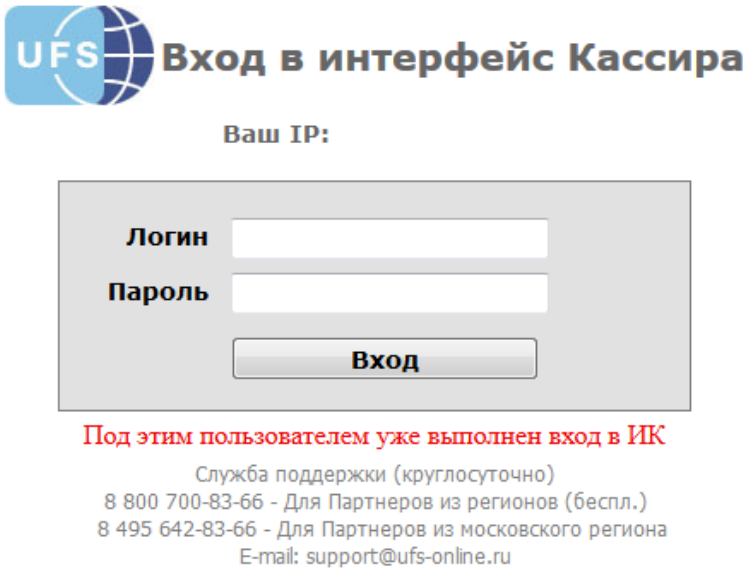
3. ОГРАНИЧЕНИЕ ПАРАЛЛЕЛЬНЫХ СЕССИЙ

В Веб-системе www.ufs-online.ru есть возможность отключить использование параллельных сеансов работы в интерфейсах под одной учетной записью (с разных ПК, с разных браузеров и т.д.).

Для включения данной функции необходимо поставить чек-бокс в соответствующее поле в настройках пользователя в Интерфейсе Администратора.



После включения будет запрещен параллельный вход в Интерфейс Кассира.



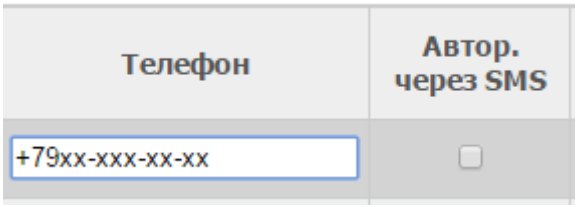
Данный функционал не позволит злоумышленнику воспользоваться чужой учетной записью с другого компьютера, например при краже пароля.

4. ИСПОЛЬЗОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

На сегодня этот вариант аутентификации является наиболее популярным и надежным.

Он является достаточно надежным барьером и позволяет свести к минимуму возможности злоумышленника даже при наличии украденного логина и пароля.

Для включения двухфакторной аутентификации необходимо в Интерфейсе Администратора в настройках пользователя включить «Авторизацию через СМС» и указать телефон, на который в дальнейшем будут приходить СМС с одноразовым паролем.



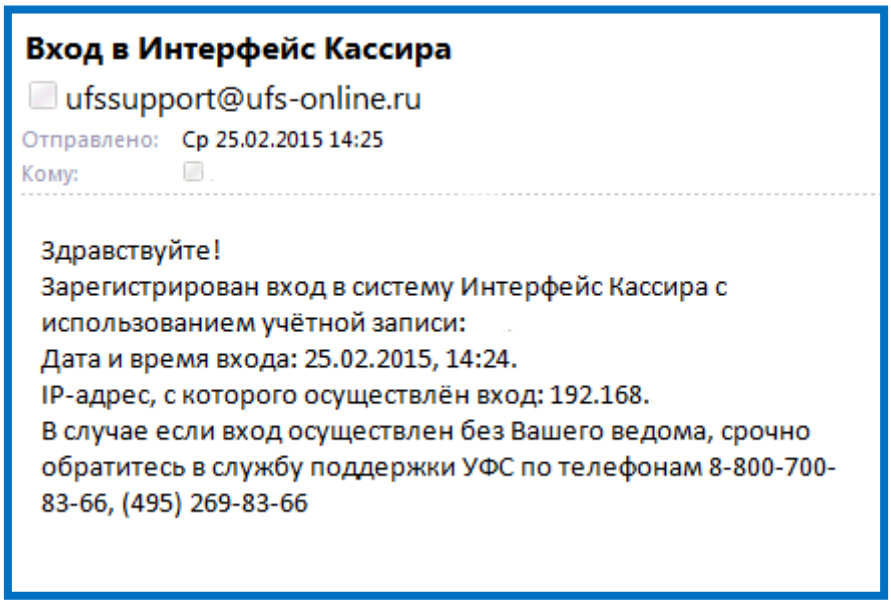
Таким образом, злоумышленник, даже зная учетные данные Кассира, не сможет войти в Веб-систему www.ufs-online.ru, не зная одноразового пароля, который будет направлен по СМС.

Также рекомендуется подключать двухфакторную аутентификацию при входе не только в Интерфейс Кассира, но и в Интерфейс Администратора.

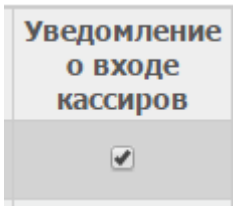
5. НАСТРОЙКА ОПОВЕЩЕНИЙ О ВХОДЕ В ИК

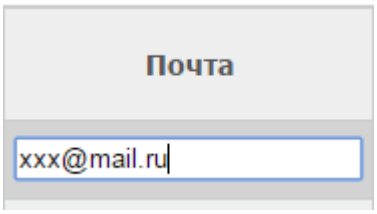
В Веб-системе www.ufs-online.ru есть функция оповещения, повышающая безопасность использования системы.

На указанный почтовый адрес отправляется уведомительное информационное письмо о каждом входе в Интерфейс Кассира с указанием даты, времени, с какого адреса осуществлен вход, и имени пользователя, под которым осуществлен вход, вида:



Для включения оповещений необходимо в настройках пользователя в Интерфейсе Администратора прописать почтовый адрес, на который посылать уведомления и поставить чек-бокс в поле «Уведомления о входе кассиров».





Данная функция позволяет оперативно реагировать на попытки несанкционированного доступа в систему, например, быстро заблокировать учетные данные пользователя.

6. НАСТРОЙКА РОЛЕЙ В СИСТЕМЕ.

В Веб-системе www.ufs-online.ru используется ролевая модель разграничения доступа, при этом права доступа пользователей системы группируются с учетом специфики их применения.

Обязательно для входа в различные Интерфейсы использовать разные учетные данные (логин, пароль, телефон, почта). Идеально – чтобы каждым интерфейсом пользовались разные сотрудники.

Интерфейс	Включить
Администратор	☐
Бухгалтер	☐
Кассир	☐
Менеджер «УФС»	☐
Супервайзер Почты	☐
Пользователь	☐
Аудит	☐

Эта функция позволяет минимизировать ущерб при краже только одной учетной записи.

7. ЗАВЕРШЕНИЕ СЕССИИ

Во всех интерфейсах системы реализована автоматическая блокировка сессии по истечении 30 минут простоя.

Данный механизм предотвращает от несанкционированного использования системы, в отсутствии легитимного пользователя.

Также необходимо блокировать систему и ПК при покидании рабочего места, и выключать ПК в конце рабочего дня или отключать его от компьютерной сети.

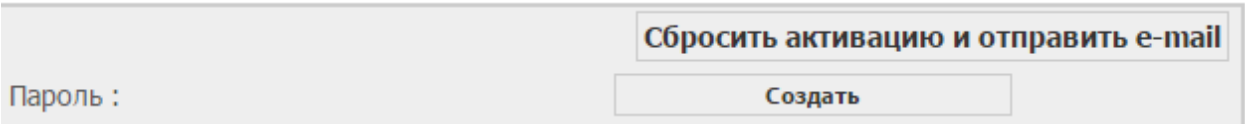
8. АКТИВАЦИЯ УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА

После создания учетной записи в Интерфейсе Администратора на указанный почтовый ящик приходит ссылка для активации учетной записи.

После перехода по ссылке предлагается ввести одноразовый СМС-код, который придёт на указанный телефон, и создать новый пароль для дальнейшей работы в Интерфейсе Администратора.

Телефон и электронный адрес Агента/Партнера указывается в договоре в Разделе 8 «Юридические адреса и банковские реквизиты сторон» в полях «Контактный телефон» и «e-mail».

При необходимости, Администратор Агента/Партнера может самостоятельно деактивировать учетную запись любого пользователя для проведения повторной активации.

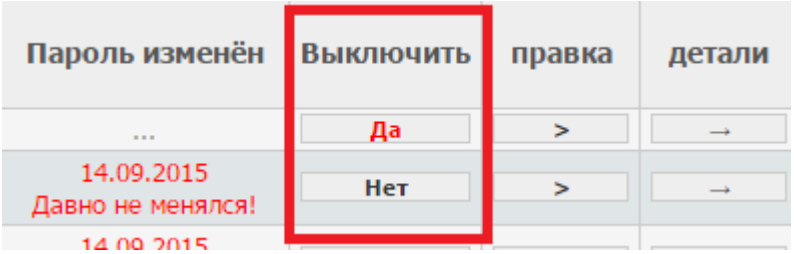


Такой способ активации по двум факторам (телефон и электронная почта) при первом входе в Веб-систему www.ufs-online.ru позволяет избежать утечки учетных данных при передаче их Агенту/Партнеру.

9. ОТКЛЮЧЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ НА ВЫХОДНЫЕ И ПРАЗДНИКИ, А ТАКЖЕ БЛОКИРОВКА НЕИСПОЛЬЗУЕМЫХ УЧЕТНЫХ ЗАПИСЕЙ

В Веб-системе www.ufs-online.ru возможно отключение или блокировка учетных записей пользователя.

Для отключения или включения определенного пользователя в Интерфейсе Администратора необходимо использовать соответствующие поля.



Данный механизм предотвращает использование легитимных учетных данных пользователя. Функция очень полезна и необходима при увольнении сотрудника, при утечке учетных данных, в праздничные и выходные дни, для находящихся в отпуске сотрудников, если необходимо временно заблокировать пользователя.

10. УСТАНОВКА ПАРОЛЯ

10.1. Длина пароля должна быть не менее 7 символов.

10.2. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

10.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, должности, даты рождения и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

10.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

10.5. Максимальный срок использования пароля должен составлять не более 90 дней.

10.6. Минимальный срок использования пароля должен составлять не менее 1 дня.

10.7. Блокировка или удаление неиспользуемых аутентификационных данных.

10.8. Внеплановая смена паролей **АБСОЛЮТНО ВСЕХ** учетных записей должна производиться в случае прекращения полномочий (увольнение, переход на другую должность или другие обстоятельства) работников, которым по роду работы были предоставлены полномочия по управлению паролями.

11. ДОПОЛНИТЕЛЬНЫЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ

11.1. Использование ТОЛЬКО лицензионного программного обеспечения, регулярная установка обновлений.

11.2. Удаление лишнего программного обеспечения, не используемого для работы.

11.3. Использование лицензионного антивирусного программного обеспечения (по возможности сертифицированного по требованиям безопасности информации) с ежедневным обновлением баз сигнатур.

11.4. Использование Межсетевого экрана на границе локальной сети. Межсетевой экран должен разрешать минимально необходимый для работы набор соединений.

11.5. Использование для входа на ПК индивидуальных учетных данных (логин, пароль) для каждого сотрудника.

11.6. Запрет на сохранение учетных данных в браузерах или иным небезопасным способом.

11.7. Блокировка входа в систему (ПК) после 3-х неправильных вводов пароля. Разблокировать может только Администратор.

11.8. Автоматическая блокировка сеанса или сессии (ПК) после простоя системы более 5 минут. Разблокировка только при повторном вводе учетных данных.

11.9. Блокировка сеанса на ПК при оставлении рабочего места.

11.10. Полное отключение питания ПК в нерабочее время.

11.11. Сбор, запись, хранение информации о событиях безопасности в течение 30 дней. Просмотр журналов регистрации событий и своевременное реагирование на подозрительные события.

11.12. Права администратора должен иметь только один сотрудник (если нет ИТ-службы), работа с правами администратора возможна только на время настройки программного обеспечения компьютера.