УТВЕРЖДАЮ
Генеральный директор
ГУП РТ «Центр информационных технологий Республики Татарстан»

_____ А.А. Валиуллин

от «06» июня 2015

№ 14-ОРД

СВОД ПРАВИЛ

по безопасной работе сотрудников органов государственной власти Республики Татарстан и органов местного самоуправления Республики Татарстан при осуществлении организации информационного взаимодействия с использованием сервисов Государственной интегрированной системы телекоммуникаций Республики Татарстан

Содержание

Используемые сокращения

В настоящем документе используются следующие сокращения:

Сокращение	Полное наименование
АИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
Пользователь	Лицо, осуществляющее информационное взаимодействия с использованием сервисов Государственной интегрированной системы телекоммуникаций Республики Татарстан

2. Общие положения

Свод правил по безопасной работе сотрудников органов государственной власти Республики Татарстан и органов местного самоуправления Республики Татарстан при осуществлении организации информационного взаимодействия с использованием сервисов Государственной интегрированной системы телекоммуникаций Республики Татарстан разработан в соответствии с Федеральным законом №149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области защиты информации.

Настоящий свод правил разработан для работников органов государственной власти Республики Татарстан, органов местного самоуправления и организаций.

Целями свода правил являются:

– регулирование работы пользователя;

– обеспечение целостности, конфиденциальности и доступности хранящейся и передаваемой информации находящейся на АРМ или ЛВС;

– соблюдение требований нормативных актов и действующего законодательства Российской Федерации в области защиты информации.

Пользователь – это лицо, осуществляющее информационное взаимодействие с использованием сервисов Государственной интегрированной системы телекоммуникаций Республики Татарстан.

Пользователь в своей работе руководствуется Сводом правил, а также иными руководящими, нормативными и регламентирующими документами в области информационной безопасности.

3. Требования к Пользователю

1. Запрещается на АРМ открывать файлы и запускать программы, полученные из непроверенных источников.
2. При получении письма от неизвестного адресата, необходимо связаться с исполнителем и уточнить происхождение файлов. В случае невозможности установить происхождение письма, необходимо его удалить, не сохраняя и не запуская приложенные файлы.
3. Необходимо выполнять регулярное (не реже 1 раза в неделю) резервное копирование важной информации, хранящейся на АРМ Пользователя.
4. Запрещается передавать свои идентификационные данные посторонним (пароли, логины).
5. Запрещается оставлять без присмотра или передавать посторонним свой ключ электронной подписи. Также не рекомендуется хранить его вместе с конвертом, так как в этом случае злоумышленник может без проблем воспользоваться этим ключом.
6. Рекомендуется не осуществлять платежные операции с использованием зарплатных банковских карт, а использовать виртуальные карты.
7. Регулярно обновлять антивирусные базы.
8. При потере ключа или при подозрении, что им кто-то воспользовался, необходимо сразу сообщить администратору информационной безопасности (лицу, ответственному за информационную безопасность) или системному администратору для организации отзыва сертификата данного электронного ключа.
9. Производить блокировку экрана АРМ при вынужденном отсутствии на рабочем месте.
10. Соблюдать требования парольной политики (Раздел «Парольная политика» Свода правил).
11. Не использовать один пароль в разных информационных ресурсах.
12. АРМ разрешается использовать исключительно в служебных целях.
13. Пользователь обязан не предпринимать попыток несанкционированного доступа к информационным ресурсам, доступ к которым ограничен.
14. Пользователь не должен использовать доступ к сети для распространения и тиражирования информации: ограниченного пользования, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.
15. Пользователь должен исключить возможность неосторожного причинения вреда техническим и информационным ресурсам организации.
16. Запрещается отключать (блокировать) средства защиты информации.
17. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с АИБ.
18. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к АИБ в исполнительном органе

государственной власти Республики Татарстан, органе местного самоуправления городского округа или муниципального района Республики Татарстан, организации.

4. Парольная политика

Правила формирования пароля:

1. пароль должен состоять не менее чем из шести символов;
2. в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например: !, $, #, %);

3. пароль не может содержать имя учетной записи Пользователя или какую-либо его часть;
4. пароль не должен включать в себя легко вычисляемые сочетания символов, простые пароли типа «123», «111», «qwerty» и им подобные, а так же ФИО и даты рождения свои и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые могут быть подобраны, основываясь на информации о пользователе;
5. не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «аааааааа»);
6. не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
7. не использовать ранее использованные пароли.
8. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
9. во время ввода пароля необходимо убедиться, что клавиатура находится вне поля зрения посторонних лиц, а также технических средств (видеокамер, фотоаппаратов).

5. Ответственность Пользователя

Каждый Пользователь несет персональную ответственность:

– за свои действия в период осуществления информационного взаимодействия с использованием сервисов Государственной интегрированной системы телекоммуникаций Республики Татарстан,

– за соблюдение требований установленных настоящим Сводом правил;

– за информацию/данные, обрабатываемые посредством его АРМ;

– за установку на АРМ программного обеспечения, модификацию или тиражирование программного обеспечения, изменение алгоритмов функционирования технических и программных средств.

За нарушение настоящего Свода правил пользователю может быть запрещен доступ к ГИСТ РТ.

Нарушение данного Свода правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством.