

УТВЕРЖДАЮ

Генеральный директор

ГУПРТ «Центр информационных технологий Республики Татарстан»



А.А. Валиуллин

от «15» июня 2015

№ 15-ОРД

РЕГЛАМЕНТ

взаимодействия при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к государственным ресурсам сторонних лиц (третьих лиц), внедрения и распространения в них вредоносных программ, проведения массированных атак типа «отказ в обслуживании», а также возможными техническими сбоями в их работе.

Содержание

1.	Используемые сокращения.....	3
2.	Терминология.....	4
3.	Общие положения.....	5
4.	Обязанности участников взаимодействия	6
5.	Ответственность участников взаимодействия.....	8

Используемые сокращения

В настоящем документе используются следующие сокращения:

Сокращение	Полное наименование
УФСБ России по РТ	Управление Федеральной службы безопасности России по Республике Татарстан
МИС РТ	Министерство информатизации и связи Республики Татарстан
ГУП РТ «ЦИТ РТ»	Государственное унитарное предприятие Республики Татарстан «Центр информационных технологий Республики Татарстан»
ОГВ РТ	Орган государственной власти Республики Татарстан
ОМСУ в РТ	Орган местного самоуправления в Республике Татарстан
АИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГИСТ РТ	Государственная интегрированная система телекоммуникаций Республики Татарстан
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
DDoS атака	Одновременная атака на систему с большого количества компьютеров с целью закрыть либо затруднить доступ пользователям системы к системным ресурсам, распределенная атака типа «отказ в обслуживании»
СЗИ	Средство защиты информации

2. Терминология

Пользователь – лицо, осуществляющее информационное взаимодействие с использованием сервисов ГИСТ РТ.

Системный администратор – работник органа государственной власти Республики Татарстан, органа местного самоуправления в Республике Татарстан, организации, который осуществляет техническую поддержку АРМ, АС, ГИС, осуществляет резервное копирование информации.

Администратор информационной безопасности – работник органа государственной власти Республики Татарстан, органа местного самоуправления в Республике Татарстан, организации, который обеспечивает функционирование установленных систем защиты информации, обновление антивирусных баз, контроль за сроками действия сертификатов СЗИ, а также осуществляет регулярный анализ защищённости информации.

Инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий, включающих в себя несанкционированные действия по уничтожению, модификации, искажению, копированию, блокированию информации и влекущих за собой вероятность создания угрозы ИБ, нарушения работы АРМ, АС и ГИС, нанесения ущерба организации.

3. Общие положения

Регламент взаимодействия при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к государственным ресурсам сторонних лиц (третьих лиц), внедрения и распространения в них вредоносных программ, проведения массированных атак типа «отказ в обслуживании», а также возможными техническими сбоями в их работе (далее – Регламент) 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 Регламент разработан для работников органов государственной власти Республики Татарстан, органов местного самоуправления в Республике Татарстан и организаций, подключенных к ГИСТ РТ.

Целью регламента является обеспечение взаимодействия органов государственной власти Республики Татарстан, органов местного самоуправления в Республике Татарстан и организаций с УФСБ России по РТ.

Задачами регламента является:

- организация деятельности работников, осуществляющих администрирование информационных систем, подключенных к ГИСТ РТ;
- регулирование работы пользователя;
- обеспечение целостности, конфиденциальности и доступности информации, находящейся на АРМ или ЛВС;
- соблюдение требований нормативных актов и действующего законодательства Российской Федерации в области защиты информации.

Пользователь, системный администратор и администратор информационной безопасности в своей работе руководствуется Регламентом, а также иными руководящими, нормативными документами и регламентирующими документами в области информационной безопасности.

Органам государственной власти Республики Татарстан необходимо в течение 10 рабочих дней информировать УФСБ России по РТ, МИС РТ, ГУП РТ «ЦИТ РТ» о принятых на работу/уволенных системных администраторах и АИБ (ФИО, должность, контактные данные).

Органам местного самоуправления в Республике Татарстан уровня муниципальный район и городской округ рекомендовать в течение 10 рабочих дней информировать УФСБ России по РТ, МИС РТ, ГУП РТ «ЦИТ РТ» о принятых на работу/уволенных системных администраторах и АИБ (ФИО, должность, контактные данные).

4. Обязанности участников взаимодействия

3.1. Обязанности пользователя:

- 3.1.1. Соблюдать требования «Свода 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», утвержденного Генеральным директором ГУП РТ «Центр информационных технологий Республики Татарстан» от 26.06.2015 №14-орд (далее – Свод правил);
- 3.1.2. Представлять свое автоматизированное рабочее место АИБ для контроля;
- 3.1.3. Выполнять требования и рекомендации АИБ и системного администратора;
- 3.1.4. Незамедлительно информировать обо всех выявленных нарушениях, связанных с информационной безопасностью АИБ и системного администратора.

3.2. Обязанности системного администратора:

- 3.2.1. Осуществлять техническую поддержку АРМ, АС, ГИС;
- 3.2.2. Обеспечивать бесперебойную работу системного программного обеспечения, серверного оборудования и АРМ пользователей;
- 3.2.3. Производить обновление антивирусных баз;
- 3.2.4. Обеспечивать резервное копирование данных (восстановление данных при необходимости);
- 3.2.5. Незамедлительно информировать АИБ обо всех выявленных нарушениях, связанных с информационной безопасностью;
- 3.2.6. Осуществлять мероприятия по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращать другие формы незаконного вмешательства в информационные ресурсы и системы (в режиме 24/7);
- 3.2.7. Выполнять требования и рекомендации АИБ.
- 3.2.8. Вести журнал инцидентов информационной безопасности (Приложение);
- 3.2.9. В кратчайшие сроки, не превышающие одного рабочего дня, предпринимать меры по восстановлению работоспособности информационных ресурсов и информационных систем. Предпринимаемые меры при необходимости согласуются с АИБ и вышестоящим руководством;
- 3.2.10. Совместно с АИБ проводить анализ зарегистрированных инцидентов информационной безопасности для выработки мероприятий (плана мероприятий) по их предотвращению.

3.3. Обязанности АИБ:

- 3.3.1. Проводить инструктаж пользователей по вопросу информационной безопасности;
- 3.3.2. Требовать от пользователей соблюдения Свода правил;

- 3.3.3. Информировать непосредственное руководство о фактах нарушений требований свода правил со стороны пользователей;
- 3.3.4. Обеспечивать функционирование установленных систем защиты информации;
- 3.3.5. Осуществлять контроль резервного копирования информации;
- 3.3.6. Контроль обновления антивирусных баз;
- 3.3.7. Осуществлять контроль за сроками действия сертификатов соответствия на СЗИ;
- 3.3.8. Осуществлять контроль ведения журнала инцидентов информационной безопасности;
- 3.3.9. Проводить раз в 6 месяцев внутренний аудит информационной безопасности;
- 3.3.10. При получении информации от пользователей, системного администратора, УФСБ России по РТ, МИС РТ, ГУП РТ «ЦИТ РТ» об инцидентах информационной безопасности, совместно с системным администратором осуществлять мероприятия по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращать другие формы незаконного вмешательства в информационные ресурсы и системы (в режиме 24/7);
- 3.3.11. Обо всех фактах инцидентах, повлекших выход из строя, либо временное приостановку АРМ, АС, ГИС (информационные ресурсы, серверное оборудование), а также о фактах несанкционированного воздействия, заражения вредоносными программами, в течение одного рабочего дня информировать УФСБ России по РТ;
- 3.3.12. Предоставлять по запросу УФСБ России по РТ, МИС РТ, ГУП РТ «ЦИТ РТ» в течение трех рабочих дней отчет об инцидентах информационной безопасности и/или копии журналов инцидентов информационной безопасности;
- 3.3.13. Совместно с системным администратором проводить анализ зарегистрированных инцидентов информационной безопасности для выработки мероприятий (плана мероприятий) по их предотвращению.

5. Ответственность участников взаимодействия

Каждый Пользователь несет персональную ответственность:

- за свои действия в период осуществления информационного взаимодействия с использованием сервисов ГИСТ РТ;
- за соблюдение требований, установленных настоящим Регламентом.

Системный администратор и АИБ несут персональную ответственность за неисполнение или исполнение не в полном объеме своих обязанностей, перечисленных в п. 3 Регламента.

Нарушение данного Регламента, 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.

**ФОРМА ЖУРНАЛА
инцидентов информационной безопасности**

№ п/п	Краткое описание инцидента ИБ	Кем обнаружен (ФИО, должность)	Дата и время обнаружения	Дата и время решения проблемы	Отметка о доведении в УФСБ России по РТ (дата, время, кто принял информацию)	Подпись системного администратора /АИБ