СОГЛАСОВАНО
Начальник Управления ФСБ
России по Саратовской области

_____ И.И. Завозяев

25 августа 2016 года

УТВЕРЖДАЮ
Вице-губернатор
Саратовской области

_____ И.И. Пивоваров

26 августа 2016 года

РЕГЛАМЕНТ
реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в информационные системы органов исполнительной власти области и органов местного самоуправления области

1. Используемые сокращения

В настоящем документе используются следующие сокращения:

Сокращение	Полное наименование
УФСБ	Управление Федеральной службы безопасности России по Саратовской области
ГПЗИ	Головное подразделение Саратовской области по технической защите информации ограниченного доступа, не отнесенной к государственной тайне, и обеспечению защиты общедоступной информации
ОИВ	Органы исполнительной власти Саратовской области
ОМСУ	Органы местного самоуправления Саратовской области
АИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИС	Информационная система
ГИС	Государственная информационная система
МИС	Муниципальная информационная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
СЗИ	Средство защиты информации

2. Термины

Пользователь - должностное лицо ОИВ, ОМСУ или подведомственных им организаций (далее – организаций), осуществляющее информационное взаимодействие с ИС, ГИС с использованием информационно-телекоммуникационной сети «Интернет».

Администратор информационной безопасности – служащий или работник организации, который осуществляет мероприятия и выполняет функции по технической защите информации, обрабатываемой в ИС, ГИС, МИС, осуществляет резервное копирование информации, обеспечивает функционирование установленных средств защиты информации, обновление антивирусных баз, контроль за сроками действия сертификатов СЗИ, а также регулярный анализ защищённости информации.

Инцидент информационной безопасности – проявление одного или нескольких нежелательных событий, включающих в себя несанкционированные действия по уничтожению, модификации, искажению, копированию, блокированию информации и влекущих за собой вероятность создания угрозы ИБ, нарушения конфиденциальности, целостности, доступности информации, работы АРМ, ИС, ГИС.

3. Общие положения

Регламент реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения (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 служащих и работников организаций при эксплуатации ГИС с использованием сети «Интернет».

Целью Регламента является обеспечение взаимодействия организаций с УФСБ, ГПЗИ.

Задачами Регламента является:

- организация деятельности служащих и работников, осуществляющих администрирование или защиту информации в ИС, ГИС подключенных к ЛВС Правительства области;
- регулирование работы Пользователей;
- обеспечение целостности, конфиденциальности и доступности информации, обрабатываемой в ИС, ГИС, МИС;
- соблюдение требований нормативных актов и действующего законодательства Российской Федерации в области защиты информации.

Пользователи и АИБ организаций в своей работе руководствуется Регламентом, а также иными руководящими, нормативными документами и регламентирующими документами в области информационной безопасности.

ОИВ необходимо в течение 10 рабочих дней информировать ГПЗИ о принятых на работу, уволенных или назначенных, освобожденных от функциональных обязанностей АИБ (ФИО, должность, контактные данные).

ОМСУ уровней муниципальный район и городской округ рекомендуется в течение 10 рабочих дней информировать ГПЗИ о принятых на работу, уволенных или назначенных, освобожденных от функциональных обязанностей АИБ (ФИО, должность, контактные данные).

4. Обязанности участников взаимодействия

4.1. Обязанности Пользователей:

4.1.1. Соблюдать требования «Правил безопасной работы служащих органов исполнительной власти области, органов местного самоуправления области при осуществлении эксплуатации информационных систем и интернет-сервисов с использованием информационно-телекоммуникационной сети «Интернет», исх. от 22.08.2016 г. №№ 01-14/1358, 01-15/1360 (далее – Правила);

4.1.2. Представлять закрепленное АРМ для контроля АИБ;

4.1.3. Выполнять требования и рекомендации АИБ;

4.1.4. Незамедлительно информировать АИБ обо всех выявленных нарушениях, связанных с информационной безопасностью.

4.2. Обязанности АИБ:

4.2.1. Осуществлять мероприятия и выполнять функции по технической защите АРМ, ИС, ГИС, МИС;

4.2.2. Обеспечивать бесперебойную работу СЗИ, установленных на серверном оборудовании и АРМ Пользователей;

4.2.3. Производить обновление антивирусных баз;

4.2.4. Обеспечивать резервное копирование данных (восстановление данных при необходимости);

4.2.5. Проводить регулярные инструктажи Пользователей по вопросу информационной безопасности;

4.2.6. Требовать от Пользователей соблюдения Правил;

4.2.7. Информировать непосредственного руководителя о фактах нарушений Правил со стороны Пользователей;

4.2.8. Обеспечивать функционирование установленных систем защиты информации;

4.2.9. Осуществлять мероприятия по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращать другие формы неправомерного вмешательства в работу информационных ресурсов и систем;

4.2.10. Вести журнал учета инцидентов информационной безопасности (Приложение);

4.2.11. Проводить не реже одного раза в 6 месяцев внутренний аудит информационной безопасности (проведение анализа защищенности ключевых элементов ИТ-инфраструктуры: внешний периметр, внутренняя инфраструктура, веб-сайты и веб-приложения);

4.2.12. Осуществлять контроль за сроками действия сертификатов соответствия на СЗИ;

4.2.13. В кратчайшие сроки, не превышающие одного рабочего дня, предпринимать меры по восстановлению работоспособности информационных

ресурсов и информационных систем;

4.2.14. При получении информации от пользователей, УФСБ, ГПЗИ об инцидентах информационной безопасности незамедлительно осуществлять мероприятия по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращать другие формы незаконного вмешательства в информационные ресурсы и системы;

4.2.15. Обо всех инцидентах, повлекших выход из строя, либо временное приостановку работы АРМ, ИС, ГИС, МИС, а также о фактах несанкционированного воздействия, заражения вредоносными программами, в течение одного рабочего дня информировать УФСБ, ГПЗИ;

4.2.16. Предоставлять по запросу УФСБ, ГПЗИ в течение трех рабочих дней отчет об инцидентах информационной безопасности и копии журналов учета инцидентов информационной безопасности;

4.2.17. Проводить анализ зарегистрированных инцидентов информационной безопасности для выработки мероприятий по их предотвращению.

5. Организация процесса реагирования на инциденты информационной безопасности

5.1.1. Основной задачей на начальном этапе реагирования является определение характера сбоев и нарушений в работе АРМ, ИС, ГИС и достоверное установление того, что выявленные нежелательные события, действия и характеристики являются действительно нарушениями, а, например, не проявлением особенностей работы программного обеспечения.

5.2. Цели организации процесса реагирования на инцидент

5.2.1. Подтвердить или опровергнуть факт инцидента.

5.2.2. Скоординировать действия при устранении последствий инцидентов.

5.2.3. При возникновении инцидентов восстановить в кратчайшие сроки работоспособность ИС, ГИС, МИС.

5.2.4. Представить детализированный отчет о произошедшем инциденте.

5.2.5. Представить рекомендации по недопущению в дальнейшем подобных инцидентов.

5.2.6. Обеспечить быстрейшее обнаружение, предупреждение инцидентов в дальнейшем путем совершенствования политики информационной безопасности, модернизации системы защиты информации.

5.2.7. Минимизировать ущерб от последствий инцидентов.

5.2.8. Провести обучение служащих ОИВ, ОМСУ процессу реагирования на инциденты информационной безопасности.

5.3. Примеры инцидентов

5.3.1. Инциденты, из-за которых получен несанкционированный доступ к информации в ИС, ГИС, МИС.

5.3.2. Утеря или кража АРМ, ноутбуков, комплектующих или носителей информации.

5.3.3. Попытки служащих ОИВ, ОМСУ получить доступ к ИС, ГИС, МИС выше имеющегося уровня доступа.

5.3.4. Попытки внутри или снаружи ИС получить несанкционированный доступ к информации (взлом ИС).

5.3.5. Потеря части информации или незавершенные транзакции.

5.3.6. Проявление действий вредоносного программного обеспечения.

5.3.7. Поврежденные сектора на жестких дисках, ошибки памяти.

5.3.8. Неверные контрольные суммы или значения хеш-функций.

5.3.9. Длительные простои в работе АРМ, ИС, ГИС, МИС в течение неприемлемого периода времени (если простой длится значительно дольше, чем оговорено в руководстве по эксплуатации или контракте об оказании услуг и не может быть устранен в течение определенного времени).

5.4. Локализация и устранение последствий инцидента

5.4.1. Определение конкретных параметров инцидента, его характера (конкретных сегментов сети, серверов, групп АРМ, приложений, затронутых компьютерной атакой).

5.4.2. Предварительный анализ действий нарушителя и сценария произошедшей (происходящей) атаки, алгоритма работы появившегося вируса и т.п.

5.4.3. Блокирование действий нарушителя (если нарушение является длящимся).

5.4.4. Блокирование (полное или частичное) работы информационной системы (сервера, базы данных, сегмента сети и т.п.) с целью недопущения дальнейших разрушительных действий, распространения вредоносных программ или утечки конфиденциальной информации.

6. Ответственность участников взаимодействия

Пользователь несет персональную ответственность:

- за свои действия в период осуществления информационного взаимодействия при эксплуатации ГИС с использованием сети «Интернет»;
- за соблюдение требований, установленных настоящим Регламентом.

АИБ несет персональную ответственность за неисполнение или исполнение не в полном объеме своих обязанностей, перечисленных в п. 4 Регламента.

Нарушение данного Регламента, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, влечет за собой дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством.

Министр области –
председатель комитета по
информатизации области **Л.Ю. Кузнецова**

Приложение
к регламенту реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в информационные системы органов исполнительной власти области и органов местного самоуправления области

ЖУРНАЛ
учета инцидентов информационной безопасности

№ п/п	Краткое описание инцидента ИБ	Кем обнаружен (ФИО, должность)	Дата и время обнаружения инцидента ИБ	Дата и время устранения инцидента ИБ	Отметка о направлении информации в УФСБ и ГПЗИ (дата, время, кто принял информацию)	Подпись АИБ