**Инструкция**

**действий при выявлении инцидентов информационной безопасности**

Настоящая Инструкция регламентирует порядок действий при выявлении инцидентов информационной безопасности (далее – инциденты ИБ).

Настоящая Инструкция подготовлена в целях минимизации последствий инцидентов ИБ, недопущения повторения инцидентов ИБ в будущем.

Настоящая Инструкция подготовлена в соответствии со следующими документами:

1) Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

2)Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

3)Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4)«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом Федеральной службой по техническому и экспортному контролю Российской Федерации от 18.02.2013 года № 21.

Настоящая инструкция не распространяется на следующие случаи:

1)осуществляется хранение, комплектование, учет и использование архивных документов, содержащих персональные данные, в соответствии   
с законодательством об архивном деле в Российской Федерации;

2)осуществляется обработка персональных данных, отнесенных   
в установленном порядке к сведениям, составляющим государственную тайну.

Требования настоящей Инструкции являются обязательными для всех

лиц, осуществляющих или Организующих обработку, защиту персональных данных.

**Выявление инцидентов безопасности и реагирование на них**

Инциденты безопасности:

1) отказ в обслуживании;

2) длительные нарушения в работе технических средств, программного обеспечения и (или) средств защиты информации;

3) нарушение правил разграничения доступа;

4) неправомерные действия по сбору информации;

5) внедрение вредоносных компьютерных программ (вирусов);

6) выявление признаков инцидентов безопасности при анализе журналов событий;

7) иные события, приводящих к реализации угроз информационной безопасности.

Источниками информации об инцидентах безопасности для ИС являются:

1) факты, выявленные сотрудниками организации;

2) результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

3) журналы и оповещения операционных систем серверов/АРМ/ ОС/гостевых ОС, антивирусной системы, системы резервного копирования   
и других подсистем безопасности;

4) обращения субъектов персональных данных с указанием инцидента безопасности;

5) сообщения ФСТЭК России;

6) сообщения ФСБ России;

7) сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

8) иные источники информации.

Основные виды инцидентов безопасности:

1) несанкционированный доступ к информационным ресурсам ИС;

2) разглашение защищаемой информации либо угроза такого разглашения;

3) превышение полномочий – несанкционированный доступ к каким-либо ресурсам и помещениям;

4) компрометация учетных записей или паролей;

5) вирусная атака или вирусное заражение;

6) сетевые атаки (отказ в обслуживании), атаки типа Man-in-the-Middle, сниффер пакетов, переадресация портов, IP-спуфинг, атаки на уровне приложений и другое.

**Обнаружение, идентификация и регистрация инцидентов безопасности**

Выявление инцидентов безопасности и реагирование на них включает   
в себя следующие мероприятия:

1) регламентация правил и процедур реагирования на инциденты безопасности, в том числе определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов безопасности;

3) своевременное информирование администратора информационной безопасности о возникновении инцидентов безопасности;

4) анализ инцидентов безопасности, в том числе определение источников   
и причин возникновения инцидентов безопасности, а также оценка их последствий;

5) принятие мер по устранению последствий инцидентов безопасности;

6) планирование и принятие мер по предотвращению повторного возникновения инцидента безопасности;

7) хранение и защита информации об инцидентах безопасности.

Обнаружение инцидентов безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов безопасности с помощью технических средств;

2) выявление инцидентов безопасности в ходе контрольных мероприятий.

При получении информации о несанкционированном воздействии на инфраструктуру ИС администратор информационной безопасности обязан убедиться, что инцидент безопасности не является результатом собственной ошибки или санкционированных действий.

Лицо, обнаружившее инцидент, должно незамедлительно, любым доступным способом, сообщить об инциденте администратору информационной безопасности, который принимает решение о необходимости информирования пользователей ИС о возникновении инцидента безопасности и дает указания по дальнейшим действиям.

Пользователи ИС, выявившие инцидент безопасности, должны незамедлительно информировать администратора информационной безопасности о возникновении инцидента безопасности в ИС.

Администратор информационной безопасности учитывает инциденты безопасности в журнале учета нештатных ситуаций в информационных системах, информирует об инциденте специалиста (подразделение) по защите информации, ответственного за защиту информации, а также при необходимости другие структурные подразделения.

Перечень действий при реагировании на инциденты безопасности, реализуемые администратором информационной безопасности совместно   
со специалистом (подразделением), ответственным за защиту информации:

1) принятие мер по устранению инцидентов безопасности;

2) анализ инцидентов безопасности, в том числе определение источников   
и причин возникновения инцидентов безопасности, а также оценка их последствий;

3) планирование и принятие мер по предотвращению повторного возникновения инцидентов безопасности.

**Планирование и принятие мер по предотвращению инцидентов безопасности**

Планирование и принятие мер по предотвращению возникновения инцидентов безопасности осуществляется администратором информационной безопасности и основывается на:

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и работников;

2) проведении мероприятий по обучению работников правилам и способам работы со средствами защиты;

3) доведении до работников норм законодательства, локальных актов по вопросам информационной безопасности и устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с лицами, принимаемыми на работу,   
и увольняющимися сотрудниками;

5) своевременной модернизации системы обеспечения информационной безопасности с учетом возникновения новых угроз информационной безопасности и при изменении требований законодательных актов и нормативных документов по защите информации;

6) своевременном обновлении ПО, в том числе ПО СЗИ и средств криптографической защиты информации.