

ПОЛИТИКА обнаружения вторжений

1 Общие положения

1.1 Настоящая Политика определяет требования к обнаружению вторжений в информационную инфраструктуру УФИЦ РАН.

2 Обнаружение вторжений

2.1 В УФИЦ РАН обеспечивается обнаружение и предотвращение вторжений, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием режима обнаружения и предотвращения вторжений на аппаратном средстве межсетевого экранирования.

2.2 На применяемом аппаратном средстве межсетевого экранирования режим обнаружения вторжений включает в себя регистрацию событий безопасности, анализ событий безопасности и распознавания компьютерных атак и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

2.3 Обнаружение (предотвращение) вторжений осуществляется на внешней границе информационной инфраструктуре УФИЦ РАН.

2.4 Права по управлению (администрированию) аппаратным средством межсетевого экранирования предоставлены только уполномоченным должностным лицам в соответствии с Политикой управления доступом.

2.5 Режим обнаружения вторжений обеспечивает реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования информационной инфраструктуры.

3 Обновление базы решающих правил

3.1 В УФИЦ РАН обеспечивается обновление базы решающих правил обнаружения вторжений.

3.2 Обновление базы решающих правил обнаружения вторжений предусматривает:

3.2.1 получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

3.2.2 получение из доверенных источников и установку обновлений базы решающих правил;

3.2.3 контроль целостности обновлений базы решающих правил.



Подлинник электронного документа, подписанного ЭП,
хранится в системе электронного документооборота
ФГБНУ Уфимского федерального исследовательского
центра Российской академии наук

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00C6211AEAAA0D5B157E47E36209026498
Владелец: Мартыненко Василий Борисович
Действителен: с 22.07.2024 по 15.10.2025