ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

о банке данных угроз безопасности информации

от 6 марта 2015 г. № 240/22/879

В соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, Федеральной службой по техническому и экспортному контролю (ФСТЭК России) совместно с заинтересованными федеральными органами исполнительной власти и организациями сформирован банк данных угроз безопасности информации.

Доступ к банку данных угроз безопасности информации осуществляется через сеть «Интернет» (адрес: www.bdu.fstec.ru). Возможен доступ через официальный сайт ФСТЭК России (раздел «Техническая защита информации», подраздел «Банк данных угроз»).

Банк данных угроз безопасности информации включает базу данных уязвимостей программного обеспечения (далее – уязвимости), а также перечень и описание угроз безопасности информации, наиболее характерных для государственных информационных систем, информационных систем персональных данных и автоматизированных систем управления производственными и технологическими процессами на критически важных объектах (далее – информационные (автоматизированные) системы).

Банк данных угроз безопасности информации сформирован в целях информационной и методической поддержки при проведении органами государственной власти и организациями работ по:

определению и оценке угроз безопасности информации в информационных (автоматизированных) системах, разработке моделей угроз безопасности информации в ходе создания и эксплуатации информационных (автоматизированных) систем;

выявлению, анализу и устранению уязвимостей в ходе создания и эксплуатации информационных (автоматизированных) систем, программно-технических средств, программного обеспечения и средств защиты информации, проведения работ по оценке (подтверждению) их соответствия обязательным требованиям;

разработке, производству и поддержанию программных (программно-технических) средств контроля защищенности информации от несанкционированного доступа.

Банк данных угроз безопасности информации предназначен для:

заинтересованных органов государственной власти, органов местного самоуправления и организаций, являющихся в соответствии с законодательством Российской Федерации обладателями информации, заказчиками и (или) операторами информационных (автоматизированных) систем;

организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию (проектированию) информационных (автоматизированных) систем;

организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по защите информации в ходе создания (проектирования) и эксплуатации информационных (автоматизированных) систем;

организаций, осуществляющих в соответствии с законодательством Российской Федерации создание программно-технических средств, программного обеспечения и средств защиты информации;

заявителей на обязательную сертификацию средств защиты информации;

органов по сертификации и испытательных лабораторий (центров), выполняющих работы по оценке (подтверждению) соответствия в отношении средств защиты информации.

Внесение информации об уязвимостях и угрозах безопасности информации (включая редактирование, изменение, наполнение (добавление новых записей)) в банк данных угроз безопасности информации осуществляется ФСТЭК России.

В банк данных угроз безопасности информации включается информация об уязвимостях и угрозах безопасности информации, полученная по результатам выявления и анализа:

сведений, опубликованных в общедоступных источниках, в том числе в информационно-телекоммуникационной сети Интернет;

сведений, полученных по результатам работ, проводимых федеральными органами исполнительной власти в рамках своих полномочий (компетенций);

сведений, поступивших из органов государственной власти, организаций и иных лиц, выполняющих работы по защите информации.

Каждой уязвимости и угрозе безопасности информации, подлежащей включению в банк данных угроз безопасности информации, присваивается идентификатор.

Идентификатор, присваиваемый уязвимости, состоит из двух групп цифр, разделенных дефисом, и имеет вид:

XXXX-XXXXX.

Первая группа цифр «XXXX» представляет собой календарный год включения уязвимости в банк данных угроз безопасности информации. Вторая группа цифр «XXXXX» является порядковым номером уязвимости в банке данных угроз безопасности информации.

Идентификатор, присваиваемый угрозе безопасности информации, состоит из буквенной аббревиатуры «УБИ» и группы цифр и имеет вид:

УБИ.XXX.

Группа цифр «XXX» представляет собой порядковый номер угрозы безопасности информации в банке данных угроз безопасности информации (от 001 до 999).

Уязвимость подлежит включению в банк данных угроз безопасности информации, если по результатам ее анализа получена и проверена информация, как минимум, по описанию уязвимости, наименованию и версии программного обеспечения, в котором возможна уязвимость, уровню опасности уязвимости.

Угроза безопасности информации подлежит включению в банк данных угроз безопасности информации, если по результатам ее анализа и проверки получена вся необходимая информация.

Включение информации в банк данных угроз безопасности информации осуществляется по мере появления (получения) сведений о новых уязвимостях и угрозах безопасности информации и их рассмотрения.

Доступ к банку данных угроз безопасности информации осуществляется в режиме просмотра (чтения) информации об уязвимостях и угрозах безопасности информации. Информация, содержащаяся в банке данных угроз, является общедоступной.

Заинтересованным органам государственной власти и организациям рекомендуется использовать информацию, содержащуюся в банке данных угроз безопасности информации, при организации и проведении всех видов работ по защите информации, установленных нормативными правовыми актами, методическими документами и национальными стандартами в области обеспечения информационной безопасности.

Лицам (исследователям), планирующим направить информацию об уязвимостях в банк данных угроз безопасности информации через раздел «Обратная связь», необходимо учитывать, что данные (фамилия и имя) исследователя, выявившего уязвимость, могут быть опубликованы в банке данных угроз. Это необходимо для анализа и организации устранения уязвимостей в конкретном программном обеспечении, в ходе которого возможно потребуются взаимодействие и совместные действия со специалистами Службы и (или) иными организациями, включая разработчиков (производителей) программного обеспечения.

В течение 2015 года ФСТЭК России планирует осуществлять мониторинг и анализ функционирования банка данных угроз безопасности, а также отработку процедур взаимодействия заинтересованных органов государственной власти и организаций по выявлению, анализу и устранению уязвимостей. По результатам указанной работы будут определены направления совершенствования и расширения функциональности банка данных угроз безопасности информации.

Начальник 2 управления
В.Лютиков