БДУ ФСТЭК – практическое использование

В рамках статьи рассмотрены основные возможности, которые специалистам по защите информации предоставляет Банк данных угроз (БДУ) ФСТЭК России, а также проведено экспресс-сравнение с альтернативными источниками информации по уязвимостям и угрозам.

Банк данных угроз безопасности информации (БДУ – www.bdu.fstec.ru), запущенный в 2015 году ФСТЭК России (Федеральная служба по техническому и экспортному контролю) и ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (Государственный научно-исследовательский испытательный институт проблем технической защиты информации), на сегодняшний день насчитывает **205** угроз и **17 391** уязвимость.

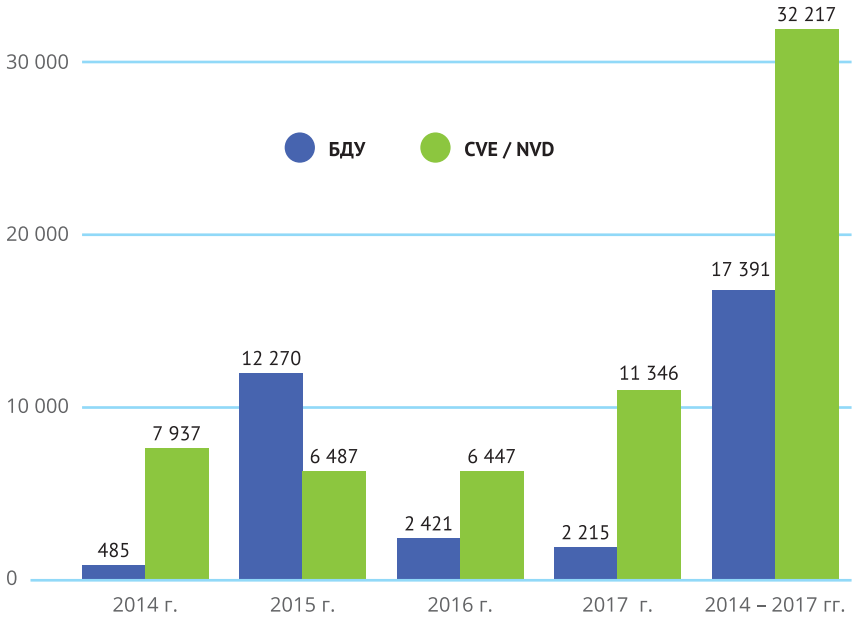
База уязвимостей и База угроз – это далеко не все возможности, которые предоставляет БДУ, однако это именно те разделы сайта, которые на практике, пожалуй, используются чаще всего.

База уязвимостей

ФСТЭК, как уже отмечалось выше, начала вести свою базу уязвимостей в 2015 году, когда в мире существовало уже более 60 различных баз схожей направленности.

Самой обширной и содержательной на тот момент была открытая независимая база Open Source Vulnerability Database (OSVDB). OSVDB насчитывала более 120 000 уязвимостей, однако 5 апреля 2016 года её деятельность была прекращена, по мнению многих – не в последнюю очередь из-за роста популярности программ Bug Bounty, позволяющих исследователям заработать деньги с помощью продажи найденных ими уязвимостей. Бесплатная публичная база уязвимостей, по всей видимости, не оправдала себя во всё более коммерциализируемом мире.

Из других крупных баз уязвимостей можно отметить популярную Common Vulnerabilities and Exposures (CVE), поддерживаемую The MITRE Corporation и являющуюся основой для американской национальной базы U.S. National Vulnerability Database (NVD). Также стоит упомянуть базы X-Force компании IBM и SecurityFocus компании Symantec, китайскую China National Vulnerability Database of Information Security (CNNVD) и японскую Japan Vulnerability Notes (JVN iPedia).



Сравнение динамики добавления новых уязвимостей в базы БДУ и CVE / NVD за последние 4 года.

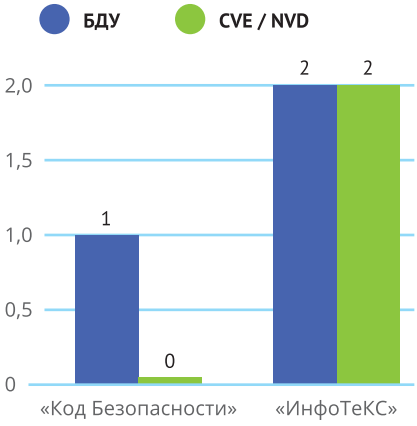
Все упомянутые и государственные, и принадлежащие частным корпорациям базы существенно превышают БДУ ФСТЭК как по количеству уязвимостей, так и по скорости обновления.

Говоря о базах уязвимостей, нельзя не упомянуть российский проект Vulners, также стартовавший в 2015 году и стремительно набирающий популярность. В некоторых источниках его называют «Google для хакера», так как Vulners автоматически собирает информацию из популярных баз уязвимостей, бюллетеней безопасности, тематических ресурсов и других источников, а также позволяет искать по ним. Из-за многообразия источников и видов представленной информации общее число записей, выдаваемых при поиске, на сегодня превышает 600 000 штук. Среди плюсов Vulners – открытый программный интерфейс (API), встроенный расширенный язык поисковых запросов и даже собственный Telegram-бот @vulnersBot.

На таком общем фоне БДУ ФСТЭК выглядит далеко не всеобъемлюще и отчасти несовременно, однако у данного источника есть два неоспоримых преимущества.

Во-первых, БДУ ФСТЭК – самая крупная база уязвимостей на русском языке. Понятные описания и понятный интерфейс дорогого стоят – на одном из мероприятий по информационной безопасности наполовину в шутку, а наполовину всерьёз из зала прозвучала фраза: «Уязвимости, опубликованные в базе ФСТЭК, для нас весомее, чем такие же, но в западных источниках».

Второй плюс БДУ ФСТЭК – ориентация в том числе на уязвимости в отечественном программном обеспечении. Уже сейчас представлены около 80 уязвимостей 11 отечественных производителей, таких как НПП «РЕЛЭКС», «Лаборатория Касперского», «ОВЕН», «1С», «1С-Битрикс» и других. Важным следствием из такой ориентации является наличие уникальных уязвимостей, которые в других базах могут быть не представлены.



Для наглядной иллюстрации были изучены уязвимости отечественных производителей средств защиты информации «ИнфоТеКС» и «Код Безопасности». Обе известные уязвимости в решениях «ИнфоТеКС» представлены и в базе CVE/NVD. Однако важная уязвимость в продукте Secret Net компании «Код Безопасности» в ней отсутствует до сих пор.

Среди других доступных для выбора, но пока не имеющих опубликованных уязвимостей на сайте БДУ ФСТЭК значатся также отечественные производители «НПО РусБИТех», «ТЕКОНГРУП», «АСКОН», «Интеллектуальные Системы Автоматизации Технологии», «Нанософт», «Новые электронные технологии», «НТЦ ИТ РОСА» и другие.

В своих публичных выступлениях сотрудники ФСТЭК заявляли, что публикуют уязвимости только после выпуска производителями соответствующих обновлений. Возможно, наличие указанных выше производителей среди доступных для выбора как раз говорит о том, что в их продуктах есть известные уязвимости, исправление которых ФСТЭК ожидает для их публикации в БДУ.

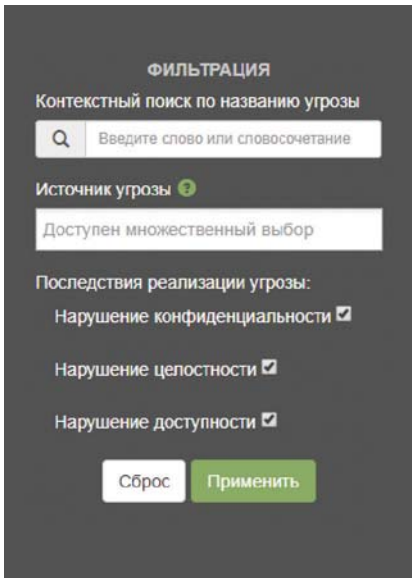
База угроз

Второй важный компонент БДУ ФСТЭК – это каталог уязвимостей. Из широко известных аналогов можно назвать разве что каталог угроз Федерального ведомства по информационной безопасности Германии: BSI IT-Grundschutz-Kataloge. Данный каталог обновляется раз в год или два, последнее обновление (версия 15) было в мае 2016 года, тогда же было заявлено, что форма подачи материала (сейчас это единый PDF-файл с 5000 страницами) будет изменена для упрощения её практического использования. Текущая версия IT-Grundschutz-Kataloge доступна на немецком и английском (черновик) языках и, помимо описания угроз, содержит общие рекомендации по нивелированию угроз (в том числе физическими, организационными и техническими мерами). Каталог отлично структурирован, имеет сквозную нотацию, а общее число описанных угроз превышает 700.

Как указано в описании БДУ ФСТЭК: *«Угрозы безопасности информации, включённые в состав банка данных угроз, не являются элементами иерархической классификационной системы угроз, а представляют собой обобщённый перечень основных угроз безопасности информации, потенциально опасных для информационных систем»*.

Каталог угроз в БДУ ФСТЭК пока позволяет искать только по названию угрозы и применять фильтры по источнику угрозы и последствиям

реализации угрозы (нарушение конфиденциальности, целостности и/или доступности).



Окно фильтрации на сайте БДУ

Равно как и для Базы уязвимостей, важнейшим преимуществом Базы угроз от ФСТЭК является детальное описание угроз на русском языке. С другой стороны, порой это описание избыточно и затрудняет, наравне с уже упомянутым отсутствием структурированности, практическое использование, так как, по сути, для каждой из 205 угроз нужно провести анализ и обосновать её актуальность либо неактуальность для конкретной информационной системы.

Так как все угрозы с их описанием и другими имеющимися полями можно просто выгрузить в виде табличного документа (для уязвимостей можно сделать то же самое), на практике работа с БДУ существенно упрощается ручным укрупнением разделов Базы угроз путём объединения схожих угроз в группы, что позволяет исключать из рассмотрения, например, все угрозы, связанные с технологиями виртуализации, если в рассматриваемой информационной системе они не применяются. Такую «доработку» БДУ обычно достаточно сделать один раз, после чего применять в своей повседневной работе, время от времени дополняя структуру новыми угрозами, публикуемыми ФСТЭК.

Дополнительные разделы и возможности

Помимо важных и полезных Базы уязвимостей и Базы угроз, сайт БДУ ФСТЭК предлагает дополнительные инструменты, которым также можно найти применение в типовой деятельности специалиста по информационной безопасности. Впрочем, справедливости ради, стоит отметить, что большинство дополнительных разделов пока скорее ближе к прототипам, чем к полноценным инструментам.

Термины и определения

Данный раздел задуман как глоссарий с официальными (выбранными из различных стандартов) определениями основных терминов и ссылкой на источник. К сожалению, раздел пока так и остался в зачаточном состоянии – 66 определений (не для всех из которых, к слову, указан источник) вряд ли можно считать хорошим подспорьем. Документация среднего размера проекта может содержать больше терминов.

Документы

Опять-таки, просто отличная задумка – собрать в одном месте (да ещё и систематизировать) всю требуемую в работе специалиста по защите информации документацию (ГОСТы, приказы, методические рекомендации и проч.), но текущая реализация снова оставляет желать лучшего: 9 документов, с поиском которых и так особых проблем не возникает. Да и выложены не сами документы, а ссылки на них. Похоже, корректнее раздел было бы назвать «Ссылки на документы».

Калькуляторы CVSS

Интерактивные калькуляторы, позволяющие, не покидая сайт ФСТЭК, быстро получить оценку CVSS – вещь удобная. Впрочем, существенным образом скопированная с калькулятора на сайте NIST идея уступает в реализации: у NIST гораздо информативнее, но зато только на английском языке.

Инфографика

Отличный раздел, который позволяет в красивом графическом представлении посмотреть топ-10 производителей, в программном обеспечении (ПО) которых обнаружено максимум уязвимостей (на первых трёх местах: свободное ПО, Red Hat, Inc. и Adobe Systems Incorporated), такой же топ-10, но уже по числу критических уязвимостей (в лидерах – та же тройка, только чуть в другом порядке) и, наконец, распределение уязвимостей по типам ошибок, уровням опасности и типам ПО.

Участники и Обратная связь

Задуманная как доска почёта таблица с информацией о частных исследователях, сообщивших об уязвимостях, содержит информацию о 17 переданных через форму обратной связи уязвимостях от 7 человек. Подраздел «Организации» заполнен логотипами тех, кто помогает ФСТЭК в наполнении базы. Опыт работы с формой обратной связи показывает, что она действующая и запросы – по крайней мере, о выявленной уязвимости – обрабатываются оперативно.

Обновления

Чтобы завершить с второстепенными разделами, стоит отметить возможность получения информации об обновлениях: непосредственно на сайте (в разделе «Новости»), через подписку на RSS-ленту и, наконец, через официальный аккаунт в «Твиттере» – @gniiiptzi

Заключение

В качестве основного пожелания дальнейшего развития Банка данных угроз к уже высказанному, пожалуй, можно было бы добавить предложение разработать соответствующие методики по работе с БДУ и, прежде всего, методику по работе с Базой угроз.

Вместе с тем, несмотря на имеющиеся недостатки, Банк данных угроз от ФСТЭК и ГНИИИ ПТЗИ является лучшим на сегодняшний день отечественным русифицированным инструментом для работы специалиста по защите информации с перечнями угроз и уязвимостей. Пусть пока не все задачи можно решить исключительно с помощью реализованных механизмов, БДУ развивается как в плане полноты охвата, так и по числу предоставляемых возможностей.

Алексей Комаров
автор блога по информационной безопасности www.zlonov.ru