ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

УДК 004.056.53
DOI: 10.22213/2410-9304-2019-2-4-10

ОРГАНИЗАЦИЯ СБОРА И ХРАНЕНИЯ ДАННЫХ ОБ ИСПЫТАНИЯХ СТРЕЛКОВОГО ОРУЖИЯ С ПОМОЩЬЮ ВЕБ-ПРИЛОЖЕНИЯ

А. Ю. Вдовин, кандидат технических наук, доцент, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия

На предприятиях, осуществляющих баллистические испытания стрелкового оружия, применяются специализированные системы для оценки параметров стрелкового оружия и боеприпасов. При этом достаточно распространены проблемы, связанные с хранением данных о проведенных испытаниях и безопасной их передачей. В связи с этим для таких предприятий целесообразно внедрение централизованной системы хранения результатов испытаний с применением современных способов защиты данных.

В статье сформулированы требования для разрабатываемой системы централизованного сбора и хранения данных о баллистических испытаниях. Для решения поставленной задачи обоснована необходимость разработки веб-приложения.

Описана предложенная концепция централизованного хранения данных об испытаниях стрелкового оружия. Обоснованы принятые решения. Предложена конкретная структура базы данных.

Созданное с использованием предложенных рекомендаций веб-приложение позволяет сохранять не только файлы с данными о конкретном испытании, но и уже обработанные результаты в виде протоколов испытаний стрелкового охотничьего и спортивного оружия. Предложенный вариант реализации приложения предоставляет возможность хранения данных об испытаниях стрелкового оружия в единой базе данных (БД) с четкой структурой, что позволяет оперативно получать доступ к необходимой информации при обеспечении высокого уровня защиты данных в соответствии с современными российскими стандартами шифрования.

Ключевые слова: веб-приложение, защита информации, испытания стрелкового оружия, база данных, TLS.

Введение

На предприятиях, осуществляющих баллистические испытания стрелкового оружия, применяются специализированные системы [1–5], использующие различные способы оценки параметров стрелкового оружия и боеприпасов.

При этом вплоть до настоящего времени в некоторых случаях результаты испытаний хранятся лишь в виде журналов, заполняемых вручную оператором. Обрабатывать такие данные достаточно неудобно, кроме того, велики сроки получения результатов конечным заказчиком.

В случае же использования автоматизированных систем данные могут сохраняться в электронном виде, но и в этом случае возникает ряд проблем, связанных с хранением информации об испытаниях в некоем унифицированном виде, а также с безопасной передачей информации заказчику. Кроме того, некоторые из предприятий, осуществляющих разработку и создание охотничьего и спортивного стрелкового оружия (как огнестрельного, так и пневматического), имеют территориально распределенную структуру, и для них чрезвычайно актуальны вопросы централизованного хранения и передачи информации об испытаниях изделий между отдельными структурными подразделениями, при этом на всех этапах получения, обработки и хранения подобной информации она должна быть надежно защищена.

В связи с этим для таких предприятий целесообразно внедрение некоей единой централизованной системы хранения результатов испытаний (как промежуточных, так и конечных), разумеется, с применением современных способов защиты данных.

Разработка системы

Были сформулированы следующие требования для разрабатываемой системы централизованного сбора и хранения данных баллистических испытаний:

1) ограничение и разграничение доступа к данным;

2) хранение информации в единой базе данных;

3) возможность быстрого обновления версий программы;

4) использование надежных средств защиты данных;

5) обеспечение возможности одновременной работы множества пользователей;

6) единый «дружественный» интерфейс для упрощения обучения персонала работе с приложением.

Разрабатываемая система, очевидно, должна включать в себя базу данных (БД) и приложение, обеспечивающее доступ к этой БД для удаленных пользователей, имеющих соответствующие права.

Подобную задачу можно было бы решить посредством реализации классической клиент-серверной компьютерной программы, но логичнее разрабатывать веб-приложение. К существенным преимуществам последнего варианта относится его независимость от конкретной операционной системы, к тому же такой вариант позволяет не заботиться об обновлении программы на каждом отдельном компьютере, т. к. само приложение хранится и запускается на одной вычислительной машине, выступающей в роли сервера (рис. 1).

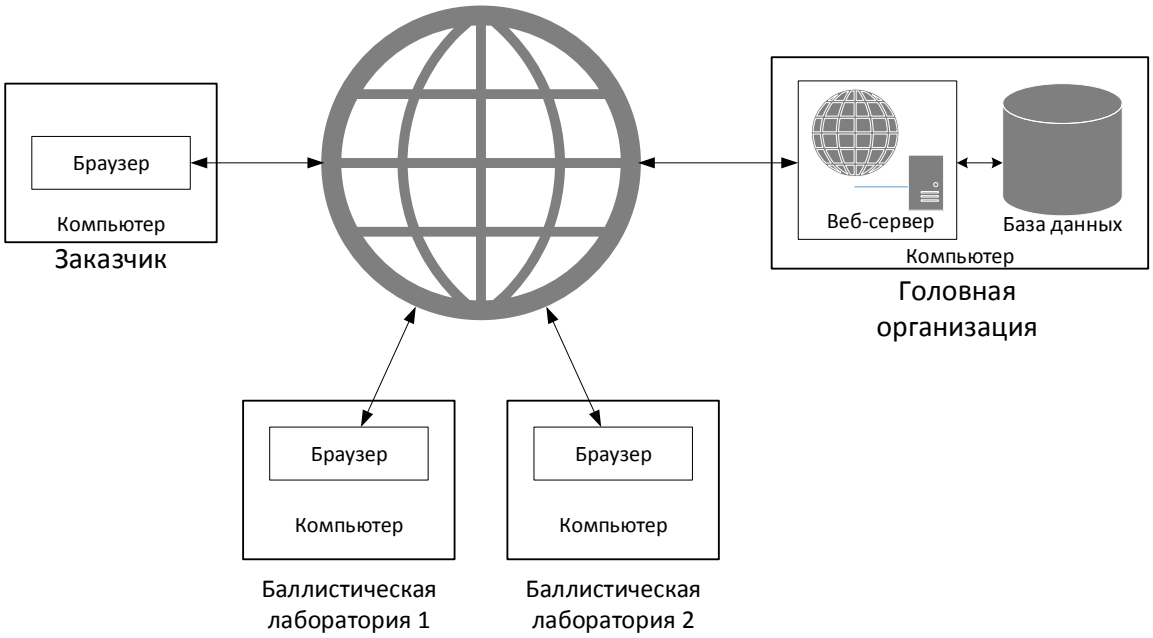

Рис. 1. Структура веб-приложения

В веб-приложении также достаточно просто обеспечить защищенную передачу данных в сети Интернет, для этой цели широко применяются криптографические протоколы SSL/TLS [6].

Предварительный анализ [7] позволил принять следующие проектные решения.

В качестве веб-сервера был выбран свободно распространяемый веб-сервер Apache. Одним из ключевых критериев выбора был принят факт поддержки большого числа вариантов контроля доступа пользователей к разделам приложения. К преимуществам можно отнести и большое число поддерживаемых ОС.

В качестве языка программирования был выбран PHP. Данный язык достаточно широко распространен, имеет большое количество фреймворков и других сторонних библиотек. Этот язык относится к категории открытого программного обеспечения, для него имеются библиотеки с поддержкой различных алгоритмов шифрования. Важное преимущество PHP заключается в его многочисленных CMS (системах управления содержимым), которые предоставляют удобные инструменты для работы с содержимым.

В качестве СУБД была выбрана PostgreSQL с открытым исходным кодом. Для работы с данной СУБД в языке PHP есть специальные функции, обеспечивающие еще один уровень защиты – исключение возможности так называемых SQL-инъекций. Данная СУБД поддерживает возможность использования протоколов SSL/TLS для передачи данных. Присутствует возможность добавления пользователей и выдачи им специальных прав на каждую таблицу. Также существует возможность хранения многомерных массивов, что принципиально важно для решения поставленной задачи, т. к. существенно ускоряет занесение данных в таблицу.

Для упрощения и ускорения разработки приложения было принято решение о необходимости использования специального программного обеспечения – фреймворка. Был выбран Yii [8] – объектно ориентированный компонентный фреймворк с подсистемой отложенной инициа-

лизации (то есть код загружается только тогда, когда он необходим). В него включены обширные возможности по контролю доступа к приложению и к его разделам, начиная от стандартного логина и пароля и заканчивая IP-адресом клиента. Yii имеет встроенные интерфейсы для работы с базами данных PostgreSQL и MySQL, обладает предустановленными наборами css-свойств и интерфейсов ввода данных, что позволяет быстро производить разработку пользовательского интерфейса.

На рис. 2 представлен реализованный интерфейс загрузки файлов.

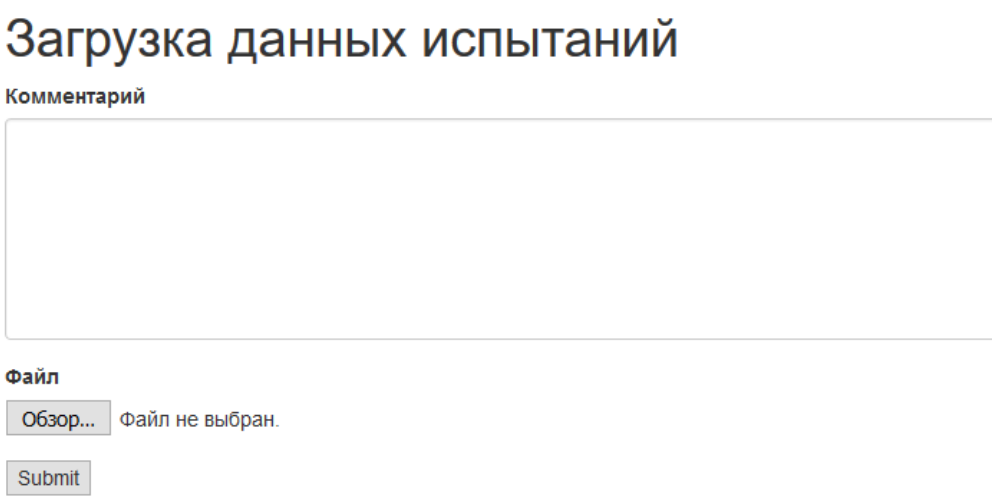

Рис. 2. Интерфейс загрузки файлов на сервер

Модели в Yii позволяют настроить фильтры вводимых данных, при этом установленные правила фильтрации, назначенные в моделях для данных, передаются на сторону клиента и не позволяют ему отправить некорректные данные, что позволяет освободить сервер от дополнительной нагрузки, связанной с проверкой корректности вводимых данных.

В качестве механизма разграничения доступа к данным было принято решение использовать контроль на основе ролей (RBAC). Данный вариант сочетает в себе преимущества мандатного и дискреционного механизмов, он позволяет выдавать права сразу группе пользователей [9]. К тому же выбранный фреймворк имеет встроенные механизмы для реализации ролевого разграничения доступа.

В БД необходимо хранить данные, необходимые для успешной аутентификации пользователей: логины и хеш-суммы паролей.

В настоящее время широко применяются хеш-функции SHA-1 и SHA-2, а до недавнего времени – MD5 [10], в России – функция хеширования по ГОСТ Р 34.11–2012. Существует и еще целый ряд хеш-функций: bcrypt, FSB, Tiger, но для них либо уже существуют известные атаки, либо серьезные исследования их стойкости криптографами не проводились. Для MD5 на данный момент известно несколько видов атак по поиску коллизий, в связи с чем он был признан небезопасным [11].

Сведем для наглядности некоторые характеристики функций SHA-1, SHA-2 и ГОСТ Р 34.11-2012 в табл. 1.

Таблица 1. Некоторые характеристики рассматриваемых хеш-функций

Параметр	SHA-1	SHA-2	ГОСТ Р 34.11-2012
Размер хеша, бит	160	224/256/384/512	256/512
Количество раундов	80	64/80	12

Размер хеша SHA-1 сравнительно невелик, и на текущий момент уже известны успешные атаки по нахождению коллизий для алгоритма [12]. Найдены потенциальные уязвимости и в алгоритме SHA-2. В связи с этим выбрана функция хеширования по ГОСТ Р 34.11–2012.

При разработке БД необходимо учесть, что на сервере должны храниться как промежуточные результаты (например, регистрация информационно-измерительной системой отдельного выстрела, полученная с использованием виртуального цифрового осциллографа в формате *.csv [2]), так и окончательные (протоколы испытания, включающие в себя сводные данные и необходимую статистическую информацию по

серии выстрелов). При этом в самой БД логичнее всего хранить ссылки на эти файлы.

Перечислим необходимые таблицы создаваемой БД: нам необходимо хранить в БД информацию для аутентификации и авторизации пользователей; персональные данные пользователей; информацию о существующих в системе ролях/правилах и о назначении отдельным пользователям конкретных ролей/правил.

Разработана следующая структура БД (рис. 3) [7].

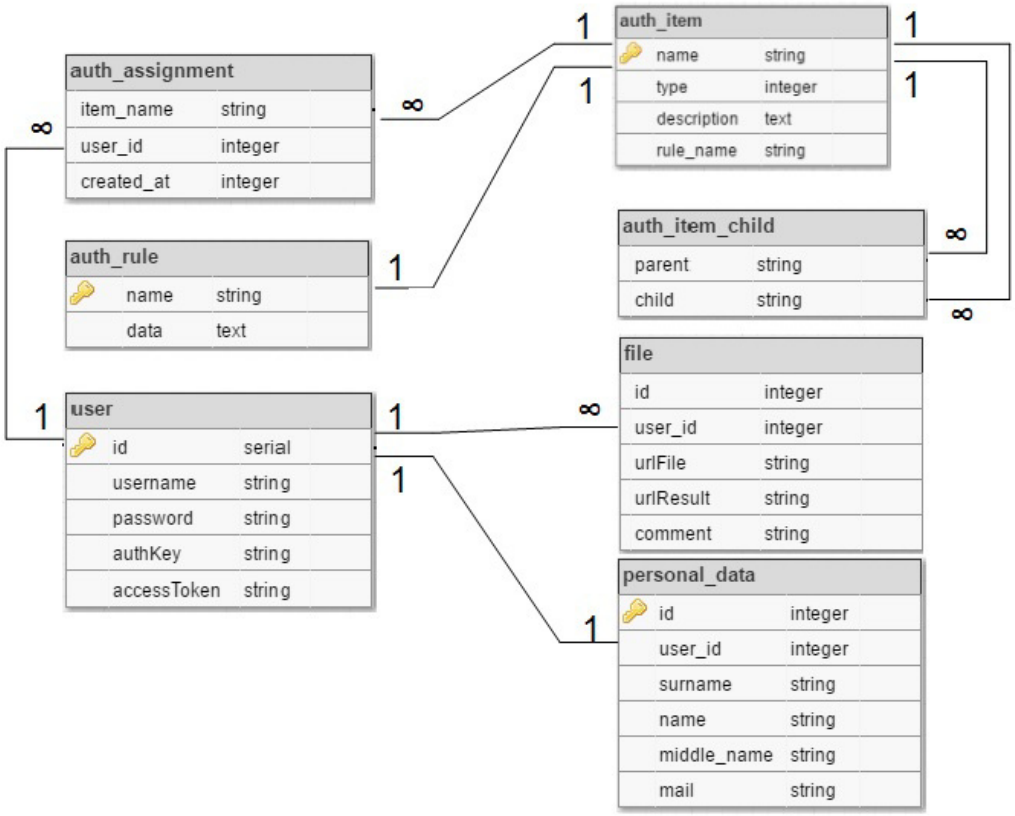

Рис. 3. Схема разработанной базы данных

На рис. 3 основными являются следующие таблицы:

1) таблица **User** содержит данные, необходимые для авторизации и аутентификации пользователей;

2) таблица **auth_item** содержит role/permission (роли/правила) и их описание;

3) таблица **auth_assignment** хранит данные о назначении пользователям role/permission;

4) таблица **file** предназначена для хранения ссылок на файлы с промежуточными результатами и протоколами испытаний стрелкового оружия;

5) таблица **personal_data** предназначена для хранения персональных данных пользователя.

Описанный вариант реализации структуры БД не претендует на оптимальность. В частности, для обеспечения большей гибкости структуры можно предложить хранение путей к файлам с данными в файлах настроек. При реализации реальной БД с большим количеством хранимых данных от разных ИИС логичным было бы хранить протоколы испытаний в отдельной директории по каждой ИИС.

Как уже отмечалось ранее, в настоящее время многие веб-приложения для обеспечения защищенной передачи информации в сети Интернет используют протокол TLS, созданный для обеспечения конфиденциальности и целостности данных при их передаче между двумя коммуникационными приложениями. TLS обеспечивает аутентификацию сторон протокола, конфиденциальность и контроль целостности передаваемых между сторонами данных. TLS встраивается в стек коммуникационных протоколов поверх транспортного уровня и обеспечивает защиту данных этого уровня. Для организации защиты используются криптографические алгоритмы, которые оформляются в виде шифронаборов (или криптонаборов). В TLS предусмотрена возможность расширения перечня криптонаборов. При использовании TLS подразумевается, что между узлами установлено надежное соединение, поэтому, например, прото-

кол не охватывает повторную отправку потерянных пакетов данных.

Модель угроз TLS предполагает, что атакующий может как угодно вмешиваться в канал связи, в том числе активно подменять пакеты и даже прерывать связь.

Ключевые задачи TLS:

1) обеспечить конфиденциальность, то есть реализовать защиту от утечек передаваемой информации;

2) обеспечить обнаружение подмены, то есть реализовать сохранение целостности передаваемой информации;

3) обеспечить аутентификацию узлов, то есть дать механизм проверки подлинности источника сообщений.

TLS является объединением нескольких субпротоколов, разбитых на два уровня. На нижнем уровне действует протокол Record (записей), который обеспечивает защищенную передачу данных, поступающих от прикладных протоколов. На верхнем уровне действуют протоколы Handshake (установление соединения), Change Cipher Spec (оповещение об изменении параметров соединения), Alert (обмен сигнальными сообщениями) и прикладные протоколы. Протокол Handshake позволяет клиенту и серверу аутентифицировать друг друга, а также согласовать используемые криптографические алгоритмы и общие ключи до того, как прикладной протокол начнет прием или передачу данных.

Чтобы начать обмен информацией по защищенному каналу, клиент и сервер должны согласовать используемый шифронабор.

В шифронабор входят:

– криптосистема, используемая для аутентификации сервера и сеансового секрета;

– шифр, который послужит для защиты передаваемых данных;

– хеш-функция, являющаяся основой для HMAC.

Шифронаборы строго фиксированы, состав закреплен в RFC, каждому приписан свой индекс в реестре IANA.

Браузеры используют встроенный комплект шифронаборов, на сервере поддерживаемые шифронаборы настраиваются администратором. Реестр IANA в настоящий момент содержит свыше 300 шифронаборов, при этом вплоть до недавнего времени TLS не поддерживал российские алгоритмы шифрования, определяемые ГОСТ.

Для решения проблемы были разработаны рекомендации Р1323565.1.020-2018 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)», которые были утверждены в августе 2018 года. Лишь в феврале 2019 года эксперты IANA одобрили внесение в реестр российских криптонаборов 0xC1,0x00 TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC, 0xC1,0x01 TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC и 0xC1,0x02 TLS_GOSTR341112_256_WITH_28147_CNT_IMIT [13].

К настоящему моменту компанией «КриптоПРО» разработан продукт СКЗИ «КриптоПро CSP» (версия 5.0) [14], реализующий протокол Transport Layer Security (TLS v. 1.0, RFC 2246) с использованием российских криптографических стандартов (применяются криптографические алгоритмы шифрования в соответствии с ГОСТ Р 34.12–2015, выработки общего ключа с аутентификацией на основе пароля SESPAKE [15], хеширования в соответствии с ГОСТ Р 34.11–2012.

Существует и еще один вариант – использование дополнительных программно-аппаратных модулей шифрования (например, МШ «Квазар» [16]), которые могут использоваться для шифрования данных по ГОСТ Р 34.12–2015, ГОСТ Р 34.13–2015 при их передаче по оптическим каналам OTN. Но стоимость внедрения подобного решения будет чрезвычайно высока.

Анализ результатов и выводы

В работе представлен ряд рекомендаций по выбору технологий, удовлетворяющих всем заданным требованиям. Предложенные решения обладают встроенными алгоритмами шифрования данных. Обеспечение безопасности данных будет происходить на всех этапах работы приложения, начиная от ввода данных пользователем и заканчивая созданием защищенного соединения с сервером БД. Контроль доступа к разделам приложения будет осуществляться на уровне веб-сервера и самого приложения, построенного на фреймворке Yii. Размещение программы в интернете обеспечивает доступ пользователей к самой последней версии приложения, а предложенный веб-сервер обеспечивает возможность одновременной работы с данными большого числа людей. Предложены пути дальнейшего совершенствования структуры созданной БД.

Созданное с использованием предложенных рекомендаций веб-приложение позволяет сохранять не только файлы с данными о конкретном испытании, но и уже обработанные результаты в виде протоколов испытаний стрелкового

охотничьего и спортивного оружия. Предложенный вариант реализации приложения предоставляет возможность хранения данных об испытаниях стрелкового оружия в единой БД с четкой структурой, что позволяет оперативно получать доступ к необходимой информации при обеспечении высокого уровня защиты данных в соответствии с современными российскими стандартами.

Библиографические ссылки

1. *Афанасьева Н. Ю.* Информационно-измерительная система на основе световых экранов для испытаний стрелкового оружия : дис. … канд. техн. наук. Ижевск, 2003.
2. *Вдовин А. Ю.* Разработка системы на основе световых экранов для определения внешнебаллистических параметров : дис. … канд. техн. наук. Ижевск, 2010.
3. *Вдовин А. Ю., Марков Е. М., Корнилов И. Г.* Современная автоматизированная система для оценки скорости перемещения затвора стрелкового оружия // Интеллектуальные системы в производстве. Ижевск: Изд-во ИжГТУ, 2017. № 3. С. 82–87. DOI: 10.22213/2410-9304-2017-3-82-87.
4. *Казаков С. В.* Разработка и исследование информационно-измерительной системы на основе акустических мишеней для испытаний стрелкового оружия на открытой местности : дис. … канд. техн. наук. Ижевск, 2002.
5. *Марков Е. М.* Разработка методик и средств контроля параметров дробового оружия с использованием телекамеры : дис. … канд. техн. наук. Ижевск, 2011.
6. The Transport Layer Security (TLS) Protocol. Version 1.2 [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc5246 (дата обращения: 04.01.2018).
7. *Логинов Я. В., Вдовин А. Ю.* Организация хранения данных об испытаниях стрелкового оружия // Информационные технологии в науке, промышленности и образовании: сб. трудов регион. науч.-техн. очно-заоч. конф. (г. Ижевск, 28 мая 2017 г.) / науч. ред. В. А. Куликов. Ижевск : Изд-во ИжГТУ имени М. Т. Калашникова, 2017. С. 148–155.
8. Yii PHP Framewowrk. [Электронный ресурс]. URL: https://www.yiiframework.com/ (дата обращения: 08.02.2019).
9. *Хорев П. Б.* Программно-аппаратная защита информации. М. : ФОРУМ, 2013. 352 с.
10. *Фергюсон Н., Шнайер Б.* Практическая криптография / пер с англ. М. : Вильямс, 2005. 424 с.
11. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc6151 (дата обращения: 04.01.2018).
12. *Stevens M., Bursztein E., Karpman P., Albertini A., Markov Ya.* The first collision for full SHA-1 [Электронный ресурс]. URL: https://shattered.io/static/shattered.pdf (дата обращения: 09.02.2019).
13. Transport Layer Security (TLS) Parameters. [Электронный ресурс]. URL: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml (дата обращения: 04.05.2019).
14. Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. [Электронный ресурс]. URL: http://clsz.fsb.ru/certification.htm (дата обращения: 09.02.2019)
15. The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol [Электронный ресурс] URL: https://tools.ietf.org/html/rfc8133 (дата обращения: 04.05.2019).
16. Системы практической безопасности [Электронный ресурс]. URL: https://systempb.ru/ (дата обращения: 04.05.2019)

References

1. Afanas'eva N.Yu. *Informatsionno-izmeritel'naya sistema na osnove svetovykh ekranov dlya ispytanii strelkovogo oruzhiya* [Information-measuring system based on light screens for testing small arms]: PhD thesis. Izhevsk, 2003 (in Russ.).
2. Vdovin A.Yu. *Razrabotka sistemy na osnove svetovykh ekranov dlya opredeleniya vneshneballisticheskikh parametrov* [Development of a system based on light screens for determining external ballistic parameters]: PhD thesis. Izhevsk, 2010 (in Russ.).
3. Vdovin A.Yu., Markov E.M., Kornilov I.G. [Modern Automated System for Evaluation of Movement Velocity of Firearm Bolt]. *Intellektual'nye sistemy v proizvodstve*, 2017, no. 3. Pp. 82-87 (in Russ.). DOI: 10.22213/2410-9304-2017-3-82-87.
4. Kazakov S.V. *Razrabotka i issledovanie informatsionno-izmeritel'noi sistemy na osnove akusticheskikh mishenei dlya ispytanii strelkovogo oruzhiya na otkrytoi mestnosti* [Development and research of an information-measuring system based on acoustic targets for testing small arms in open areas]: PhD thesis. Izhevsk, 2002 (in Russ.).
5. Markov E.M. *Razrabotka metodik i sredstv kontrolya parametrov drobovogo oruzhiya s ispol'zovaniem telekamery* [Development of methods and means of controlling parameters of shotguns using a camera]. PhD thesis. Izhevsk, 2011 (in Russ.).
6. The Transport Layer Security (TLS) Protocol. Version 1.2 Available at: https://tools.ietf.org/html/rfc5246 (accessed 04.01.2018).
7. Loginov Ya.V., Vdovin A.Yu. *Organizatsiya khraneniya dannykh ob ispytaniyakh strelkovogo oruzhiya* [Organization of storage of test data on small arms]. *Informatsionnye tekhnologii v nauke, promyshlennosti i obrazovanii: sb. trudov region. nauch.-tekhn. ochno-zaoch. konf.* [Proc. Information technology in science, industry and education]. 2017, pp. 148-155 (in Russ.).
8. Yii PHP Framewowrk. Available at: https://www.yiiframework.com (accessed 08.02.2019).

9. Khorev P.B. *Programmno-apparatnaya zashchita informatsii* [Software and hardware information protection]. Moscow, FORUM, 2013, 352p. (in Russ.).

10. Fergyuson N., Shnaier B. *Prakticheskaya kriptografiya*. [Practical cryptography]. Moscow, Vil'yams Publ., 2005, 424 p. (in Russ.).

11. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. Available at: https://tools.ietf.org/html/rfc6151 (accessed 04.01.2018).

12. Stevens M., Bursztein E., Karpman P., Albertini A., Markov Ya. The first collision for full SHA-1. Available at: https://shattered.io/static/shattered.pdf (accessed: 09.02.2019).

13. Transport Layer Security (TLS) Parameters. Available at: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml (accessed 04.05.2019).

14. *Tsentr po litsenzirovaniyu, sertifikatsii i zashchite gosudarstvennoi tainy FSB Rossii* [Center for licensing, certification and protection of state secrets of the FSB of Russia]. Available at: http://clsz.fsb.ru/certification.htm (accessed 09.02.2019) (in Russ.).

15. The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol Available at: https://tools.ietf.org/html/rfc8133 (accessed 04.05.2019).

16. *Sistemy Prakticheskoi Bezopasnosti* [Practical Security Systems]. Available at: https://systempb.ru (accessed 04.05.2019) (in Russ.).

* * *

Collection and Storage of Data on Small-Arms Testing by Web-Application

A. Yu. Vdovin, PhD in Engineering, Associate Professor, Kalashnikov ISTU

At enterprises carrying out ballistic tests of small arms, specialized systems are used to assess the parameters of small arms and ammunition. At the same time, problems related to the storage of test data and their safe transfer are quite common. In this regard, for such enterprises it is advisable to introduce a centralized system for storing test results using modern data protection methods.

This paper states the set of requirements for the developed system of centralized collection and storage of ballistic test data. To solve this problem, the necessity of developing a web application is justified.

The proposed concept of centralized storage of data on tests of small arms is described. The taken decisions are justified. A specific database structure is proposed.

The web application developed using the proposed recommendations allows you to save data files about a specific test, as well as processed results in the form of test reports of small-arms hunting and sporting weapons. The proposed implementation of the application provides the ability to store data on testing small arms in a single database with a clear structure that allows you to quickly access the necessary information while ensuring a high level of data protection in accordance with modern Russian encryption standards.

Keywords: web application, information security, small arms tests, database, TLS.

Получено: 16.05.19