УДК 34.06

Лабутин Николай Григорьевич
Labutin Nikolay Grigor'evich

кандидат технических наук, доцент, доцент кафедры математики, информатики и информационных технологий
Нижегородская академия МВД России (603950, Нижний Новгород, Анкудиновское шоссе, 3)

candidate of sciences (technical), associate professor, associate professor of faculty of mathematics, computer science and information technologies
Nizhny Novgorod academy of the Ministry of internal affairs of Russia (3 Ankudinovskoye shosse, Nizhny Novgorod, 603950)

E-mail: ko_kol@mail.ru

Смирнов Сергей Александрович
Smirnov Sergey Aleksandrovich

преподаватель кафедры математики, информатики и информационных технологий
Нижегородская академия МВД России (603950, Нижний Новгород, Анкудиновское шоссе, 3)

lecturer of faculty of mathematics, computer science and information technologies
Nizhny Novgorod academy of the Ministry of internal affairs of Russia (3 Ankudinovskoye shosse, Nizhny Novgorod, 603950)

E-mail: ser.smir@yandex.ru

К вопросу о защите информационных ресурсов общего пользования в сети «Интернет»

To a question on protection of information general purpose resources in a network the «Internet»

В статье рассмотрены некоторые юридические и технические аспекты проблемы обеспечения безопасности информации в информационных ресурсах общего пользования. В частности, проанализированы актуальные в настоящее время угрозы информационной безопасности информационных ресурсов общего пользования в сети «Интернет». На основании этого приведены рекомендации по организации защиты информации этих ресурсов, а также способы и средства защиты информационных ресурсов в сети «Интернет», рекомендуемые авторами статьи для повышения эффективности и надежности их защиты.

Ключевые слова: безопасность информации, информационные ресурсы Российской Федерации общего пользования, защита информации, защита Web-ресурсов, уязвимости Web-ресурсов, мониторинг защищенности Web-систем.

In clause presents some legal and technical aspects of a problem of a safety of the information in information general purpose resources are considered. In particular, threats of information safety of information general purpose resources in a network the «Internet» are analysed actual now. On the basis of it recommendations for the organization of protection of the information of these resources, and also ways and means of protection of information resources in the networks the «Internet» recommended authors of clause (article) for increase of efficiency and reliability of their protection are given.

Keywords: safety of the information, information resources of the general purpose Russian Federation, protection of the information, protection of Web-resources, vulnerability of Web-resources, monitoring of security of Web-systems.

Одно из направлений применения современных информационных технологий — информационные ресурсы общего пользования в сети «Интернет». Это направление в настоящее время динамично развивается и имеет популярность у широких масс людей в связи с возможностью удаленного использования таких сервисов и услуг, как государственные услуги (уплата налогов, коммунальные платежи и т. д.), интернет-торговля, интернет-платежи, системы «Клиент-Банк», реклама услуг или деятельности компании в сети «Интернет» и др. Так как названные услуги и сервисы используют открытые телекоммуникации и общедоступные компьютерные сети, то существует проблема защиты информации и информационных систем, составляющих эти ресурсы.

Вопросам защиты информации и информационных ресурсов общего пользования, соответствен-

но, их правовому регулированию в нашей стране уделяется повышенное внимание, что подтверждается достаточно большим количеством нормативных правовых актов разного уровня, принятых за последнее время.

Представим только основные нормативные правовые акты, затрагивающие правовое регулирование именно вопросов обеспечения безопасности информационных ресурсов общего пользования в сети «Интернет»:

— Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации»;

— Федеральный закон от 7 июля 2003 года № 126-ФЗ (ред. от 21.07.2014) «О связи» (с изм. и доп., вступ. в силу с 21.10.2014);

— Федеральный закон от 21 июля 2014 года № 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства»;

— Федеральный закон от 3 декабря 2011 года № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»;

— постановление Правительства РФ от 31 июля 2014 года № 744 «Об утверждении Правил информирования граждан (физических лиц) об ограничении доступа к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и функционирование которых обеспечивается организатором распространения информации в информационно-телекоммуникационной сети “Интернет”»;

— постановление Правительства РФ от 31 июля 2014 года № 742 «Об отдельных полномочиях Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

— постановление Правительства РФ от 14 сентября 2012 года № 928 (ред. от 21.07.2014) «О базовых государственных информационных ресурсах» (вместе с «Требованиями к порядку формирования, актуализации и использования базовых государственных информационных ресурсов», «Правилами формирования, актуализации и использования реестра базовых государственных информационных ресурсов»);

— приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрировано в Минюсте России 31.05.2013 № 28608);

— приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31 августа 2010 года «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» (зарегистрировано в Минюсте РФ 13.10.2010 № 18704).

Согласно указанным документам определены общие положения и требования по защите государственных и иных информационных ресурсов общего пользования. Так как сфера применения нормативных правовых актов по данному направлению достаточно сложна, наукоемка и технологична, то существуют определенные технические особенности исполнения требований нормативных документов.

Далее рассмотрим подробнее эти технические особенности.

Уязвимостям подвержены и аппаратные и программные составляющие интернет-ресурсов. Наиболее опасны уязвимости в способах и средствах защиты Web-ресурсов, так как их выявление происходит, как правило, случайным образом или с помощью независимых специалистов, тестирующих безопасность тех или иных Web-ресурсов, инструментальных средств Web-разработки, вообще программного обеспечения за вознаграждение от их владельцев по программе Bug Bounty [1]. То есть наличие в Web-ресурсе уязвимости может обнаружиться в любое время и практически непредсказуемо.

Уязвимости в способах и средствах защиты Web-ресурсов, уязвимости самого программного обеспечения Web-ресурсов (Web-сервера, библиотек и т. д.) неизбежны, так как не бывает идеального в плане безопасности программного обеспечения.

Так, последние нашумевшие уязвимости этого класса [2; 3; 4; 5]:

1. Heartbleed (CVE-2014-0160) — ошибка в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно считывать некоторые данные из памяти на сервере или на клиенте, в том числе идентификационные данные для извлечения секретного (закрытого) ключа сервера.

OpenSSL — это самое популярное криптографическое решение для шифрования передаваемых данных в Web-серверах. Большинство Web-серверов в Интернете используют это приложение. Распространенность OpenSSL связана с тем, что оно поставляется с открытыми исходными кодами. В апреле 2014 года обнаружилась очередная уязвимость (CVE-2014-0160) в расширении протокола TLS, которое включено в OpenSSL и называется Heartbeat («сердцебиение»).

Указанная уязвимость позволяет перехватывать запросы между клиентами и сервером во время «сердцебиений», таким образом, удаленно считывать некоторые данные из памяти сервера. Соответственно, Web-ресурсы, использующие протокол HTTPS для защиты информации и базирующиеся на веб-серверах на основе OpenSSL, могут быть уязвимы.

2. Уязвимости к SQL-инъекциям.

Например, уязвимости в стандартных скриптах Drupal (программное обеспечение, является системой управления контентом (CMS), то есть системой управления сайтами, распространяется на бесплатной основе по лицензии GPL и лежит в основе большинства Web-сайтов). Такая уязвимость позволяет выполнить произвольный SQL-запрос

на сайте [6] (сменить пароль для админа, включить PHP-фильтр и добавить произвольный PHP код в одну из нод (нода — базовый элемент в структуре содержимого Drupal)).

3. Уязвимости в командной оболочке Bash, позволяющей писать скрипты для Web-приложений. В дополнение к выявленной уязвимости в Bash (CVE-2014-6271) и уязвимости, основанной на обходе исправления, устраняющего первую уязвимость (CVE-2014-7169), исследователи безопасности выявили еще три уязвимости, вызванные ошибками в реализации кода разбора функций. Так как разбор функций производится в Bash для всех переменных окружения, данные уязвимости также могут быть легко эксплуатированы через формирование специального содержимого, попадающего в переменные окружения [7]. Уязвимости в Bash в последнее время обнаруживаются весьма интенсивно и многие эксперты прогнозируют [8], что не все проблемы устранены. Для комплексной проверки систем на подверженность атакам Shellshock (в том числе и уязвимостям в Bash) уже разработан универсальный скрипт [9].

Классические способы и средства, применяемые для защиты Интернет-ресурсов, передаваемой по сети информации и межсетевых взаимодействий, в таких случаях не спасают от реализации угроз безопасности информации.

Поэтому для надежной защиты информационных ресурсов общего пользования необходимо руководствоваться Требованиями о защите информации, содержащейся в информационных системах общего пользования, утвержденными совместным приказом ФСБ РФ № 416 и ФСТЭК РФ № 489 от 31 августа 2010 года.

Согласно этим требованиям необходимо применять только сертифицированные ФСБ России классические средства защиты Web-ресурсов, такие как средства криптографической защиты информации, антивирусные средства и другие программы обнаружения вредоносного программного обеспечения, средства обнаружения вторжений и другие средства контроля доступа к информации, межсетевые экраны [10].

В приказе ФСБ РФ № 416 и ФСТЭК РФ № 489 также определено обязательное проведение организационных и технических мероприятий по защите информационных ресурсов общего пользования, направленных на недопущение реализации всех видов угроз информационной безопасности этих ресурсов.

К указанным мероприятиям относятся [10]:

— оперативная локализация и ликвидация неблагоприятных последствий нарушения порядка доступа к информации;

— обязательная запись всего сетевого трафика при обращении к государственным информационным ресурсам и его хранение не менее десяти дней для того, чтобы можно было осуществить оперативно-разыскные мероприятия по факту злонамеренного действия;

— применение классических способов технической и программно-технической защиты информационных систем общего пользования и защиты от несанкционированного доступа к помещениям, в которых они находятся;

— регистрация действий обслуживающего персонала и пользователей;

— частичное или полное (в зависимости от класса системы) резервирование технических и программных средств, дублирование носителей и массивов информации;

— использование сертифицированных систем обеспечения гарантированного электропитания (источников бесперебойного питания);

— осуществление мониторинга их защищенности уполномоченным подразделением ФСБ России;

— введение в эксплуатацию только после направления оператором информационной системы общего пользования в ФСБ России уведомления о готовности ввода информационной системы общего пользования в эксплуатацию и ее соответствии вышеупомянутым Требованиям.

Отмеченные в требованиях приказа ФСБ РФ № 416 и ФСТЭК РФ № 489 мероприятия по мониторингу защищенности и введению в эксплуатацию информационной системы общего пользования после проверки ФСБ России предназначены для выявления и оперативного устранения уязвимостей всех уровней: программного обеспечения Web-ресурсов и средств их защиты, при межсетевых взаимодействиях и при передаче данных по каналам связи.

Анализируя требования приказа ФСБ РФ № 416 и ФСТЭК РФ № 489, отметим следующие ключевые моменты.

При разработке Web-ресурса используется программное обеспечение, подверженное угрозам безопасности, в нем периодически выявляют уязвимости. Защитные средства, например программные и программно-аппаратные продукты, использующие криптозащищенные протоколы передачи данных HTTPS, FTPS с использованием SSL/TLS, межсетевые экраны, системы обнаружения вторжений, антивирусные программы, системы анализа защищенности, тоже подвержены уязвимостям.

Поэтому, во-первых, средства защиты должны быть сертифицированы ФСБ России по определенному уровню обеспечения безопасности.

Во-вторых, для защиты от уязвимостей Web-ресурсов необходимо отслеживать информацию об обнаруженных уязвимостях и оперативно принимать меры к их устранению. Как правило, эти меры заключаются в применении к уязвимому программному обеспечению разработанных исправлений (патчей). Для государственных информационных ресурсов общего пользования эти функции должно выполнять уполномоченное подразделение ФСБ России.

В-третьих, при эксплуатации информационных ресурсов необходимо осуществлять мониторинг их защищенности от других видов угроз.

Тем более, кроме требований приказа ФСБ РФ № 416 и ФСТЭК РФ № 489, мониторинг (контроль) предписывают общие Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК № 17 от 11 февраля 2013 года, в котором сказано, что «...контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляется на этапе разработки системы защиты информации информационной системы, в процессе внедрения системы защиты информации информационной системы, в ходе эксплуатации аттестованной информационной системы» [11].

В некоторых организациях, в том числе государственных, уделяется недостаточно внимания к указанным выше ключевым моментам в обеспечении информационной безопасности информационных ресурсов общего пользования, требования приказов ФСБ РФ № 416 и ФСТЭК РФ № 489, а также приказа ФСТЭК № 17 от 11 февраля 2013 года исполняются формально.

Необходимо четко представлять, что основная масса атак на защищенные информационные ресурсы сети «Интернет» возможна из-за уязвимостей в их программном обеспечении и средствах защиты [12]. Поэтому выполнение ключевых правил по защите информации, таких как:

— применение проверенных на отсутствие недекларированных возможностей Web-серверов и другого программного обеспечения функционирования информационных ресурсов общего пользования, а также программных инструментальных средств разработки Web-приложений:

— применение только сертифицированных средств защиты;

— постоянный мониторинг (контроль) защищенности информационных ресурсов на этапе разработки, создания, ввода в эксплуатацию и их использования;

— применение средств адекватного и быстрого реагирования на обнаруженные угрозы безопасности;

— использование механизмов восстановления работоспособности системы и приведения информационных ресурсов в исходное состояние является залогом безопасного использования информационных ресурсов общего пользования в сети «Интернет».

Способы мониторинга защищенности автоматизированных систем известны и представлены в национальных стандартах Российской Федерации, утвержденных для добровольного применения:

— ГОСТ Р ИСО/МЭК 15408-2009 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;

— ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»;

— ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», идентичный международному стандарту ИСО/МЭК 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»;

— ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».

Применительно к контролю защищенности информационных ресурсов сети «Интернет» авторами предлагаются следующие как традиционные, так и специфичные способы и средства мониторинга защищенности:

— средства анализа защищенности информационной системы, имитирующие во время ее работы различные виды атак;

— средства обнаружения вторжений (атак) для анализа системных событий и сетевого трафика на предмет обнаружения атак и реализующих различные ответные действия на попытки атак (программные и программно-аппаратные системные и сетевые сканеры);

— программные и программно-аппаратные средства и компоненты для предотвращения атак на защищаемые ресурсы;

— организационные мероприятия, составляющие политику и процедуры реагирования на атаки — отражение атак и последующее восстановление системы;

— мероприятия по определению критичных ресурсов в системе, надежности схемы размещения средств защиты и другие инфраструктурные решения;

— использование единого защищенного центра управления системой мониторинга.

По твердому убеждению авторов статьи, безусловное применение указанных способов и средств защиты информации позволяет значительно повысить общий уровень информационной безопасности государственных и иных информационных ресурсов в сети «Интернет».

Примечания

1. Big Bounty — это программа финансового вознаграждения, получаемого независимыми исследователями, находящими уязвимости в программном обеспечении того или иного производителя.

2. URL: https://www.emaro-ssl.ru/blog/heartbleed/

3. URL: habrahabr.ru/post/218609/

4. URL: www.drupal.ru › Форумы › Техподдержка Drupal › Безопасность

5. URL: xakep.ru/drupal-sql-injection/

6. URL: http://www.drupal.ru/node/113136

7. URL: http://www.opennet.ru/opennews/art.shtml?num=40702

8. URL: http://arstechnica.com/security/2014/09/still-more-vulnerabilities-in-bash-shellshock-becomes-whack-a-mole/

9. URL: https://github.com/hannob/bashcheck

10. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования: приказ ФСБ РФ № 416 и ФСТЭК РФ № 489.

11. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК № 17 от 11 февраля 2013 года.

12. *Лабутин Н.Г.* Некоторые способы поиска и определения местонахождения злоумышленников в сети Интернет. Математические методы и информационно-технические средства: материалы X Всероссийской научно-практической конференции. Краснодар, 2014.

Notes

1. Big Bounty is a program of the financial compensation received by independent researchers, finding vulnerability in the software of this or that manufacturer.

2. URL: https://www.emaro-ssl.ru/blog/heartbleed/

3. URL: habrahabr.ru/post/218609/

4. URL: www.drupal.ru

5. URL: xakep.ru/drupal-sql-injection/

6. URL: http://www.drupal.ru/node/113136

7. URL: http://www.opennet.ru/opennews/art.shtml?num=40702

8. URL: http://arstechnica.com/security/2014/09/still-more-vulnerabilities-in-bash-shellshock-becomes-whack-a-mole/

9. URL: https://github.com/hannob/bashcheck

10. About the statement of requirements about protection of the information contained in information general purpose systems: the order of FSB of the Russian Federation № 416 and FSTEC of the Russian Federation № 489.

11. About the statement of requirements about protection of the information which are doing not make the state secret, contained in the state information systems: order FSTEC № 17 from February, 11, 2013.

12. *Labutin N.G.* Some ways of search and definition of location of malefactors on the Internet. Mathematical methods and information technical means: materials X of the All-Russian scientific and practical conference. Krasnodar, 2014.