УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-35-38

ОСОБЕННОСТИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

Софья Васильевна Степанова
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (913)459-34-90, e-mail: stepanova.sofya@mail.ru

Никита Алексеевич Стрихарь
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (996)387-72-77, e-mail:strihar.nikita@mail.ru

В статье рассматриваются особенности выбора средств защиты информации я государственных информационных систем. Рассмотрены основные виды СЗИ, которые использовались на территории России раньше, а также средства, используемые сейчас. Приведены результаты работ, проведенных ФСТЭК и ФСБ России, относительно введения классификации СЗИ и мер, которые предпринимаются оператором ГИС. Определены тенденции развития и создания новых средств защиты информации.

Ключевые слова: информационная безопасность, средства защиты информации, государственные информационные системы.

CHOICE OF MEANS OF PROTECTION OF INFORMATION IN STATE INFORMATION SYSTEMS

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, Russia, 630108, Associate Professor, Department Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

SofyaV. Stepanova
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, Russia, 630099, Bachelor of Information Security, phone: (913)459-34-90, e-mail: stepanova.sofya@mail.ru

Nikita A. Strigari
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, Russia, 630099, Bachelor of Information Security, phone: (996)387-72-77, e-mail: strihar.nikita@mail.ru

The article discusses the features of the choice of information security tools for state information systems. The main types of SPI, which were used on the territory of Russia before, as well

as the means used now, are considered. The results of work, carried out by the FSTEC and FSB of Russia, on the introduction of the classification of SPI and measures taken by the GIS operator are presented. Tendencies of development and creation of new means of information protection are defined.

Key words: information security, means of information protection, state information systems.

Развитие науки и техники не останавливается. Это обусловлено тем, что люди стараются найти более продуманные, современные и выгодные решения. Данная тенденция распространяется и на сферу обеспечения защиты информации. Ежедневно появляются новые вирусы, совершаются различного рода хакерские атаки и взломы. Чтобы обезопасить систему, специалист по информационной безопасности обязан разбираться в тенденциях и новинках в своей сфере деятельности. Также, он должен грамотно подходить к выбору средств защиты информации, учитывая цели, особенности и возможности организации. Это касается и особенностей выбора средств защиты информации в государственных информационных системах.

Применение средств защиты информации существенно повышает уровень защиты от несанкционированного доступа. Однако, реализовать необходимый уровень защищенности возможно только при использовании сертифицированных средств защиты информации. В данной работе, разобраны проблемы выбора средств защиты информации, на основе существующих требований ФСТЭК России.

Раньше существовал ограниченный набор средств защиты информации (СЗИ). Туда входили средства вычислительной техники (СВТ) – программные и технические элементы систем обработки данных, способные функционировать самостоятельно или в составе других автоматизированных систем (АС) [5]. Существуют следующие виды средств защиты информации: технические средства и системы в защищенном исполнении, технические средства защиты информации от несанкционированного доступа (НСД) (замки, пломбы), программные средства защиты информации от НСД (антивирусные программы), защищенные программные средства обработки информации (программные средства автоматизированных систем управления), программно-технические средства защиты информации, специальные средства защиты от идентификации личности (средства защиты от дактилоскопической экспертизы) [1].

Существует семь классов защищенности СВТ от несанкционированного доступа к информации, для государственных информационных систем подходит пятый класс. Он отличается наличием дискреционного управления доступом: возможностью устанавливать права доступа пользователей к различным ресурсам. Следующим пунктом в процессе обеспечения защищенности информации является установка межсетевых экранов – средств, реализующих контроль за информацией, поступающей и выходящей из АС. Для дифференциации требований к функциям безопасности межсетевых экранов выделяются шесть классов защиты. В отношении государственных информационных систем (ГИС) рассматриваются 4 и 5 классы защищенности [3].Также для каждой

ГИС разрабатываются и утверждаются технические условия, которые могут включать в себя: требования к составу технических средств и операционной системе, наличие модуля доверенной загрузки, антивирусного решения и так далее.

Данные требования к средствам защиты информации, разработанные в начале 90-х годов, уже устарели, так как на тот момент не существовало документов, регулирующих выполнение тех требований. Начиная с 2011 года ФСТЭК России начал реализацию деятельности, направленной на изменение подходов к защите информации. Так, например, для государственных информационных систем были установлены три класса защищенности, а также требования к каждому из них. Класс защищенности определяется в зависимости от уровня значимости информации, обрабатываемой в ИС и ее масштаба. В приказе ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 15 февраля 2017 г. № 27) приведен состав мер по защите информации для каждого класса защищенности информационных систем [2].

Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия: формируются требования к защите информации, разрабатывается и внедряется система защиты информации для ИС, проводится аттестация ИС. ФСТЭК выпустил ряд документов, систематизирующих классификацию СЗИ, а также описывающих тот или иной класс. Приказами ФСТЭК России были утверждены требования к системам обнаружения вторжений, межсетевым экранам, средствам антивирусной защиты, средствам контроля съемных машинных носителей, введена классификация операционных систем для обеспечения защиты информации. ФСБ России, определила классы криптографических СЗИ и средств защиты электронной подписи [4]. На данный момент существует государственный реестр сертифицированных СЗИ, поддерживаемый ФСТЭК России. Аналогичный перечень сертифицированных СЗИ имеет и ФСБ России в рамках своей компетенции.

Здесь необходимо помнить, что надежную защиту информации, обеспечит комплексное решение, включающие соответствующие средства защиты.

Так как веб-сервисы и их структура постоянно развиваются, на этой почве возникла потребность в создании новых решений по защите информации. Одним из таких решений стал WebApplicationFirewall (WAF) – экран для защиты веб-приложений.

Продвинутые модели WAF могут анализировать XML, JSON и другие протоколы современных порталов и мобильных приложений. Это позволяет противодействовать обходу межсетевого экрана, что является важным, так как большое количество людей имеет доступ к ГИС. В качестве примера можно привести портал «Госуслуги», для регистрации на котором гражданину необходимо вводить личные данные. В этом случае использование WAF в роли СЗИ поможет предотвратить большое количество проблем. В качестве другого примера можно привести использование личного кабинета на сайте банка. Пользователь заходит на сайт, проходит там аутентификацию, а в другой вкладке открывает ресурс, который оказывается зараженным. JavaScript, загрузившийся в другом

окне, может запросить информацию о переводе денежных средств и браузер предоставит все необходимые параметры для осуществления финансовой транзакции, так как сеанс связи пользователя с банком еще не окончится. Таким образом можно выявить слабые стороны в алгоритме аутентификации. Проблему можно избежать, если для каждой формы, содержащейся на странице сайта, будет генерироваться уникальный токен. Некоторые WAF могут самостоятельно внедрять подобную защиту в веб-формы и защищать, таким образом, клиента – а вернее, его запросы, данные, URL и cookie-файлы. В ходе работы WAF запускается основной компонент защиты – машинное обучение, которое характеризуется способностью понимать группы протоколов и зависимостей, свойственных для веб-приложений, которые строятся над прикладными протоколами http/https. Таким образом формируется список допустимых идентификаторов доступа [6].

Межсетевой экран Positive Technologies Application Firewall, предназначенный для защиты от кибератак, успешно прошел сертификационные испытания ФСТЭК России. Данный межсетевой экран стал первым решением в классеWAF, подтвердившим соответствие требованиям технических условий и руководящих документов по четвертому уровню контроля отсутствия недекларированных возможностей. Наличие сертификата означает, что данный межсетевой экран может применяться в государственных информационных системах до первого класса защищенности включительно (в соответствии с приказом ФСТЭК России от 11.02.2013 № 17) и ИСПДн до первого уровня защищенности включительно (согласно приказу ФСТЭК России от 18.02.2013 № 21) [7].

В настоящее время идет большая работа по изменению требований к средствам защиты информации. Каждый год документально оформляются новые виды средств защиты, с целью обеспечить безопасность всех применяемых информационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ ФСБ РФ от 13.11.1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

2. Приказ ФСТЭК РФ от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»(ред. от 15.02.2017 г. № 27).

3. Приказ ФСТЭК РФ от 9.02.2016 г. № 9 «Требования к межсетевым экранам».

4. Приказ ФСТЭК РФ от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

5. ФСТЭК РФ. «Руководящий документ. Решение председателя Гостехкомиссии России от 30.03.1992 г.».

6. Чем защищают сайты, или зачем нужен WAF? [Электронный ресурс] – Режим доступа: https://habr.com/company/pt/blog/269165/.

7. PT ApplicationFirewall сертифицирован ФСТЭК России [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/43455/.