УДК 004.056.53

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ИНФОРМАЦИОННО-ПОИСКОВЫМИ СИСТЕМАМИ

Щекочихин О.В., канд. техн. наук, доц., зав. кафедрой защиты информации Костромского государственного университета

Синкевич Е.А., аспирант ФГБУН ВИНИТИ РАН

В статье анализируются работы российских и зарубежных авторов, посвященные анализу, сравнению и оценке автоматизированных информационно-поисковых систем с точки зрения информационной безопасности пользователей. Поиск научно-технической информации – распространенное явление, особенно при проектировании и производстве высокотехнологичных изделий. При использовании известных ресурсов, содержащих научно-техническую информацию, необходимо учитывать особенности рабочего места ученого, конструктора, технолога в организации, выпускающей наукоемкую продукцию. Предлагается система сравнительной оценки информационно-поисковых систем по базовым элементам, их критериям и оценочным показателям. Делается вывод о состоянии нормативной базы по оценке информационно-поисковых систем. Представлены критерии и показатели оценки угроз информационной безопасности в процессе поиска научно-технической информации. Рассмотрены наиболее популярные уязвимости web-приложений – межсайтовый скриптинг, кликджекинг, cookie-файлы. Показаны технологии организации атак, даны рекомендации по защите рабочего места пользователя информационно-поисковой системы.

Ключевые слова: информационно-поисковая система, информационная безопасность, критерий оценки информационной безопасности, показатель оценки информационной безопасности.

ВВЕДЕНИЕ

Безопасность информационно-поисковых систем (ИПС) их владельцы и разработчики отдают на откуп профильным специалистам, которые, в свою очередь, разъясняют программно-аппаратные причины уязвимостей и связанные угрозы, технологию их реализации и предлагают пользователям рекомендации по защите от атак злоумышленников, но не формулируют критерии безопасности ИПС. Согласно ГОСТ Р 53114–2008, критерий обеспечения информационной безопасности (ИБ) организации – это показатель, на основании которого оценивается степень достижения целей ИБ. Данная группа критериев зависит как от стандарта и политики ИБ, реализуемой в ИПС, так и от компетенций пользователя в области ИБ. Работа поисковых систем и электронных библиотечных систем (ЭБС) достаточно коммерциализирована. Поисковые системы зарабатывают деньги, показывая пользователю рекламу, а электронные библиотеки – предоставляя платный доступ к своим ресурсам, для чего ЭБС регистрируют (создают учетную запись) пользователей. В дальнейшем идентификация пользователя для получения доступа в личный кабинет осуществляется по логину и паролю. При этом их политикой конфиденциальности не предусмотрены контроль и ответственность за сайты третьих лиц, на которые пользователь может перейти по ссылкам, доступным на стартовых страницах. Механизм выявления недекларированных возможностей контента третьих лиц со стороны ИПС отсутствует.

Согласно ГОСТ Р 50922–2006, угроза безопасности информации – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Критериями безопасности информации служат выполнение организационных и технических мероприятий, вызывающих доверие со стороны пользователя к обеспечению ИБ; наличие или отсутствие уязвимостей в программно-аппаратных средствах ИПС, обеспечивающих ИБ.

На наш взгляд, требования пользователя к безопасности информации при работе с ИПС должны включать следующие критерии:

- объем персональных и других данных, циркулирующих в системе, показателями которых являются обязательные персональные данные, предоставляемые поль-

зователем при регистрации, и объем данных, передаваемых автоматически серверам сайта в процессе их использования;

- контроль и ответственность за сайты третьих лиц, куда пользователь может перейти по ссылкам, доступным на сайте ИПС. Показателями в данном случае служат наличие (отсутствие) контроля за сайтами третьих лиц, на которые пользователь может перейти по ссылкам, и наличие (отсутствие) ответственности ИПС за сайты третьих лиц, на которые пользователь может перейти по ссылкам;
- наличие (отсутствие) рекламы, показателями которых являются – количество рекламы со стороны ИПС во время сеанса поиска информации, возможность отключения рекламы на все время сеанса поиска информации и возможность отключения каждого рекламного баннера во время сеанса поиска информации.

С учетом вышеизложенного для анализа и оценки ИПС пользователем предлагается следующая система требований, их критериев и показателей оценки безопасности ИПС (табл. 1).

Критерии и показатели оценки угроз информационной безопасности в процессе поиска научно-технической информации

КРИТЕРИИ ОЦЕНКИ ИПС	ПОКАЗАТЕЛЬ КРИТЕРИЯ
Объем персональных и других данных пользователя, циркулирующих в системе	Обязательные персональные данные, предоставляемые пользователем при регистрации (создании учетной записи) и в процессе использования сервисов
	Объем данных, передаваемых автоматически серверам сайта
Контроль и ответственность за сайты третьих лиц, на которые пользователь может перейти по ссылкам, доступным на сайте ИПС	Наличие контроля за сайтами третьих лиц, на которые пользователь может перейти по ссылкам
	Наличие ответственности ИПС за сайты третьих лиц, на которые пользователь может перейти по ссылкам
Наличие (отсутствие) рекламы	Количество рекламы со стороны ИПС во время сеанса поиска информации
	Возможность отключения рекламы на все время сеанса поиска информации
	Возможность отключения каждого рекламного баннера во время сеанса поиска информации

СИСТЕМНОЕ ПРЕДСТАВЛЕНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОИСКЕ НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ

Ключевой аспект решения проблемы безопасности ИТ – выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ. Авторы, характеризующие в своих работах различные поисковые системы, рассматривают их преимущественно со стороны требований эффективности и удобства использования. При этом, на наш взгляд, недостаточное внимание уделяется критериям, отражающим требование пользователей к ИПС со стороны ИБ. Эта группа критериев зависит как от стандарта и политики ИБ, реализуемой в ИПС, так и от компетенций пользователя в области ИБ.

Поисковая система может быть эффективной и удобной, но при этом ей свойственны уязвимости безопасности, которые активизируются вследствие преднамеренных или случайных действий при использовании ИПС. Предполагается, что злоумышленники будут пытаться нарушить политики безопасности как для получения незаконной выгоды, так и для незлонамеренных, но тем не менее опасных действий. Нарушители могут также случайно активизировать уязвимости безопасности, нанося вред ИПС как организации, так и пользователю. Все это может обернуться значительными потерями.

Риски, угрозы и оценки соответствия ИПС требованиям безопасности информации в той или иной мере рассматриваются в работах [1–9]. В работе [1] авторы отмечают, что «эксплуатация сервисов сети Интернет, не говоря уже

о IP-адресе шлюза, через который пользователи подключаются к сети несет в себе определенные риски ИБ» – вероятность реализации угрозы ИБ. На первый взгляд, проблема защиты информации и обеспечение информационной безопасности при поиске НТИ не является существенной, риски для пользователя ИПС отсутствуют либо минимальны. Создается впечатление, что защищать нужно только базу данных, а это – зона ответственности собственников информационных ресурсов. Однако детальный анализ возможных рисков показал, что они могут быть достаточно существенными. Имеющиеся работы дают представление о возникающих угрозах при поиске НТИ. Появление недокументированных возможностей программных продуктов и использование их злоумышленниками определяются следующими факторами:

1. Современные программные продукты создаются командой разработчиков, поэтому увеличивается риск ошибок интеграции отдельных компонентов и модулей в единый продукт.
2. Существует возможность использовать известные уязвимости популярных операционных систем.
3. Особенности языков и сред разработки определяют уязвимости и возможные векторы атаки злоумышленников.
4. Случайные ошибки пользователей влекут за собой нарушение безопасности информации.

Рассмотрим две группы наиболее распространенных уязвимостей и атак на их основе, которым подвержены ИПС – межсайтовый скриптинг и кликджекинг. Межсайтовый скриптинг [2] позволяет злоумышленнику внедрить собственный сценарий в код web-страницы путем обхода ограничений безопасности браузера. Можно выделить три типа подобных уязвимостей: постоянный, непостоянный, возникающий непосредственно в сценарии. Метод, существующий более 15 лет, постоянно совершенствуется и модернизируется. Рейтинг опасности таких уязвимостей может варьироваться в зависимости от важности данных, хранящихся на уязвимом сайте, и существующих механизмов защиты. Уязвимости межсайтового скриптинга – опасность высокой степени, поскольку есть возможность изменить модель сайта. Целями атакующего могут быть изменение настроек, кража данных пользователей, в частности, данных файлов cookie, размещение ложной рекламы, хищение токенов форм для проведения атак другого рода и т. д.

Кликджекинг [3] заключается в том, что пользователь, совершая переход на легитимную страницу, на самом деле переходит по ссылке, сформированной злоумышленником. Цель атаки с использованием кликджекинга – заставить пользователя сайта выполнить действия на другом ресурсе – целевом. Обычно эта атака выполняется путем сокрытия пользовательского интерфейса целевого веб-сайта и организации видимого пользовательского интерфейса таким образом, чтобы пользователь не знал, что совершает действия на целевом сайте.

Одна из разновидностей кликджекинга – маскировка курсора. Пользователь считает, что совершает одно действие, а на самом деле – другое. Маскировка курсора в системах Mac OS X с использованием кода Flash, HTML и JavaScript также может привести к шпионажу веб-камеры и выполнению вредоносных приложений, позволяющих выполнять вредоносное ПО на компьютере захваченного пользователя.

Для защиты от атак кликджекинга необходимо выполнять следующие настройки:

1. Включать HTTP-заголовок X-Frame-Options во все веб-страницы пользователя, что предотвратит размещение его сайта в рамке. Данная настройка требует доступа к конфигурации веб-сервера и языку сценариев на сервере.
2. Перемещать элементы на своих страницах.
3. Включать одноразовый код в URL-адрес важных страниц.
4. Выполнять Framebuster Javascript – механизм проверки кода Javascript на предмет обнаружения.
5. Устанавливать фильтр для нежелательной почты, поскольку атаки с помощью кликджекинга обычно начинаются с обмана пользователя по электронной почте путем рассылки поддельных или специально созданных электронных писем для посещения вредоносного сайта.

На сегодняшний день не существует идеального решения для предотвращения кликджекинга – методы совершенствуются по принципу «снаряд – броня». Несмотря на это, наиболее эффективными средствами защиты от таких атак являются X-Frame и FrameBuster Javascript [4].

Еще одна популярная потенциально опасная web-технология – использование cookie файлов [5]. Наличие в cookie логинов и паролей пользователя делает их потенциальной целью злоумышленников. Для cookie файлов характерен ряд недостатков, среди которых самые значимые – низкий уровень безопасности, хранение cookie в простом текстовом формате, необходимость настройки веб-браузера.

Существует несколько вариантов атак на cookie. Первый – кража cookie – это XSS-атака или межсайтовый скриптинг, применяется для атаки на веб-сайты с целью похищения данных пользователей. Злоумышленник внедряет вредоносный код на веб-сайт; пользователь посещает веб-сайт и активирует вредоносный код; вредоносный код похищает cookie пользователя и передает их на веб-сервер злоумышленника.

Второй вариант атаки на cookie файлы – их подмена. От кражи отличается тем, что при передаче cookie файлов на веб-сервер злоумышленник не перехватывает их, а вносит соответствующие изменения непосредственно в их содержимое. Третий вариант – физический доступ к данным – вид атаки, реализуемой только при непосредственном контакте с ПК жертвы. Злоумышленник копирует cookie файлы пользователя и переносит их на внешний накопитель; злоумышленник переходит на необходимый ресурс с украденными cookie; предоставляется полный доступ к данным жертвы. Для защиты пользовательских данных в cookie от вышеперечисленных атак рекомендуется выполнять следующие действия [6]:

1. Использовать защищенные соединения (SFTP, HTTPS).
2. Не переходить на сомнительные веб-ресурсы.
3. Не сохранять персональные данные на веб-ресурсах при использовании публичных сетей Wi-Fi.
4. Своевременно удалять cookie и очищать кэш браузера.
5. Регулярно изменять пароли в аккаунтах.
6. Обновлять браузер и антивирусное ПО.
7. Настраивать использование cookie браузерами.
8. Применять механизм приватных вкладок [6].

При работе с ИПС посредством мобильных приложений риски информационной безопасности существенно возрастают, что обусловлено наличием уязвимостей следующих категорий:

1. Нарушение контроля доступа.
2. Сбои в криптографии.
3. Внедрение кода.
4. Небезопасный дизайн.
5. Небезопасная конфигурация.
6. Уязвимые и устаревшие компоненты.
7. Ошибки идентификации и аутентификации.
8. Нарушение целостности данных и ПО.
9. Журнал безопасности и сбои мониторинга.
10. Подделка запросов со стороны сервера (SSRF).

Сравнение рейтингов основных уязвимостей приложений и потенциальных угроз для пользователя OWASP [7] топ-10 2016 года и 2021-го показывает, насколько значительные изменения. По мере развития информационных технологий появляются новые уязвимости, а с ними и риски безопасности информации для пользователя. Доминирование и изменение значимости категорий в большей степени связано с ростом зависимости современного мира от информационных технологий, значительным увеличением количества компьютеров у населения и, как следствие, ростом киберпреступности. Один из факторов увеличения количества уязвимостей, а с ними и рисков безопасности информации для пользователей, – рост числа приложений для мобильных устройств [8], дублирующих функции (электронную почту, аккаунт в соцсети, личный кабинет банковских, госуслуг и др.) стационарных домашних и офисных компьютеров, с тем же логином и паролем.

ЗАКЛЮЧЕНИЕ

Как показал анализ информационно-поисковых систем для поиска научно-технической информации, существуют две группы угроз. Первая связана с незаконным обращением с персональными данными, например, учетными, паспортными, номерами банковских карт и т. п. Это может нанести ущерб непосредственно пользователю. Вторая группа угроз обусловлена профессиональной деятельностью пользователя. Злоумышленник может контролировать информационные потребности работника организации, сами запросы, и результаты поиска могут косвенно говорить о коммерческом результате, который пытается получить организация, тем самым раскрываются коммерческая тайна или стратегические направления развития организации [9, 10].

Таким образом, при поиске информации о научных исследованиях и опытно-конструкторских работах необходимо осуществлять ряд мероприятий, направленных на обеспечение информационной безопасности рабочего места.

Обеспечение безопасности пользователя поисковых систем требует более пристального внимания и активных мероприятий в соответствии с представленными в статье категориями угроз.

Список использованных источников и литературы

1. Мазов Н.А., Ревнивых А.В., Федотов А.М. Классификация рисков информационной безопасности // Вестник НГУ. Серия: Информационные технологии. 2011. Т. 9, вып. 2 © Н. 2011. ISSN 1818-7900.
2. Элхади А. М. Полное пособие по межсайтовому скриптингу // SecurityLab.ru [Электронный ресурс]. 11.12.2012. – URL: https://www.securitylab.ru/analytics/432835.php%20-%20XSS?R=1 (дата обращения 19.12.2021).
3. Clickjacking Attacks and How to Prevent Them Перевод: Andrea Chiarelli Атаки кликджекинга (clickjacking) и как их предотвратить. [Электронный ресурс] – https://webdevblog.ru/ataki-klikdzhekinga-clickjacking-i-kak-ih-predotvratit / (дата обращения 13.01.2022)

4. Дрюков В.В. Эволюция SOC: как профессиональные хакеры заставили поменять подход к ИБ-защите. https://www.securitylab.ru/analytics/527815.php (дата обращения 21.12.2021).
5. Меньщиков Р.Д., Чудинова Е.В., Москвин В.В. Курганский государственный университет, Курган COOKIE: Принципы работы и безопасность использования. 2017.
6. Cookie: что нужно знать? [Электронный ресурс] // Kaspersky lab Daily. Режим доступа: https://www.kaspersky.ru/blog/cookie-chto-nuzhno-znat/979/ (дата обращения: 22.12.2021).
7. Open Web Application Security Project® (OWASP) – открытый проект онлайн-сообщества по обеспечению безопасности приложений, все материалы доступны бесплатно на веб-сайте некоммерческой организации OWASP® Foundation. [Электронный ресурс] – https://proglib.io/p/chto-takoe-top-10-owasp-i-kakie-uyazvimosti-veb-prilozheniy-naibolee-opasny-2021-09-09 (дата обращения 24.01.2022)
8. Артамонов В. А. Безопасность мобильных устройств, систем и приложений. [Электронный ресурс] http://itzashita.ru/wp-content/uploads/2015/04/Bezop_mobil_Artamonov.pdf (дата обращения 24.01.2022)
9. Закутнев С.Е., Рязанов А.А. Использование стандартизации и технического регулирования в современной межгосударственной военно-экономической конкуренции // Информационно-экономические аспекты стандартизации и технического регулирования. 2021. № 1 (59). С. 17–21.
10. Глебова Е.В., Макаренко Д.В. Разработка модели проекта «создание информационно-справочной системы работы в ФГИС «Меркурий» / Международная научная конференция: «Стандартизация и техническое регулирование: современное состояние и перспективы развития» // Информационно-экономические аспекты стандартизации и технического регулирования. 2020. № 6 (58). С. 255–270.

THE PROBLEM OF INFORMATION SECURITY WHEN WORKING WITH INFORMATION RETRIEVAL SYSTEMS

Schekochikhin O.V., Ph.D., associate professor, Head of the Department of Information Security Kostroma State University

Sinkevich E.A., graduate student Russian Institute of Scientific and Technical Information of the RAS

The article analyzes the works of Russian and foreign authors dedicated to the analysis, comparison and evaluation of automated information retrieval systems in terms of information security of users searching for scientific and technical information. Searching for scientific and technical information is becoming a widespread phenomenon, especially in the design and production of high-tech products. When using the most well-known resources with scientific and technical information, it is necessary to take into account the peculiarities of the workplace of a scientist, designer, technologist, in the organization producing high-tech products. A system of comparative evaluation of information retrieval systems by basic elements, their criteria and evaluation indicators is proposed. The conclusion about the state of the regulatory framework for the evaluation of information retrieval systems is made. Criteria and indicators of information security threats assessment in the process of scientific and technical information retrieval are shown. The most popular vulnerabilities of web-applications – cross-site scripting, clickjacking, cokie-files – have been considered. Technologies of attacks organization are shown and recommendations are given to protect workplaces of users of information retrieval systems from them.

Keywords: *information retrieval system, information security, information security evaluation criteria, information security evaluation index.*

References

1. Mazov N. A., Revnivyh A.V., Fedotov A.M. Klassifikaciya riskov informacionnoj bezopasnosti. Vestnik NGU. Seriya: Informacionnye tekhnologii. 2011. Tom 9, vypusk 2 © N. 2011. ISSN 1818-7900.
2. Elhadi A. M. Polnoe posobie po mezhsajtovomu skriptingu // SecurityLab.ru [Elektronnyj resurs]. 11.12.2012. – URL: https://www.securitylab.ru/analytics/432835.php%20-%20XSS?R=1 (data obrashcheniya 19.12.2021).
3. Clickjacking Attacks and How to Prevent Them Perevod: Andrea Chiarelli Ataki klikdzhekinga (clickjacking) i kak ih predotvratit'. [Elektronnyj resurs] - https://webdevblog.ru/ataki-klikdzhekinga-clickjacking-i-kak-ih-predotvratit/ (data obrashcheniya 13.01.2022)
4. Dryukov V.V. Evolyuciya SOC: kak professional'nye hakery zastavili pomenyat' podhod k IB-zashchite. https://www.securitylab.ru/analytics/527815.php (data obrashcheniya 21.12.2021).
5. Men'shchikov R.D., CHudinova E.V., Moskvin V.V. Kurganskij gosudarstvennyj universitet, Kurgan COOKIE: Principy raboty i bezopasnost' ispol'zovaniya. 2017.
6. Cookie: chto nuzhno znat'? [Elektronnyj resurs] // Kaspersky lab Daily. Rezhim dostupa: https://www.kaspersky.ru/blog/cookie-chto-nuzhno-znat/979/ (data obrashcheniya: 22.12.2021).
7. Open Web Application Security Project® (OWASP) – otkrytyj proekt onlajn-soobshchestva po obespecheniyu bezopasnosti prilozhenij, vse materialy dostupny besplatno na veb-sajte nekommercheskoj organizacii OWASP® Foundation. . [Elektronnyj resurs] – https://proglib.io/p/chto-takoe-top-10-owasp-i-kakie-uyazvimosti-veb-prilozheniy-naibolee-opasny-2021-09-09 (data obrashcheniya 24.01.2022)
8. Artamonov V. A. Bezopasnost' mobil'nyh ustrojstv, sistem i prilozhenij. [Elektronnyj resurs] http://itzashita.ru/wp-content/uploads/2015/04/Bezop_mobil_Artamonov.pdf (data obrashcheniya 24.01.2022)
9. Zakutnev S.E., Ryazanov A.A. Ispol'zovanie standartizacii i tekhnicheskogo regulirovaniya v sovremennoj mezhgosudarstvennoj voenno-ekonomicheskoj konkurencii // Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya. 2021. № 1 (59). Pp. 17–21.
10. Glebova E.V., Makarenko D.V. Razrabotka modeli proekta «sozdanie informacionno-spravochnoj sistemy raboty v FGIS «Merkurij» / Mezhdunarodnaya nauchnaya konferenciya: «Standartizaciya i tekhnicheskoe regulirovanie: sovremennoe sostoyanie i perspektivy razvitiya» // Informacionnoekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya. 2020. № 6 (58). Pp. 255–270.