DOI: 10.18137/RNU.V9187.22.03.P.169 УДК 004.056.53

А.Р. Газизов

АППАРАТНО-ПРОГРАММНЫЕ И ОРГАНИЗАЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ РЕСУРСОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПУТЕМ SQL-ИНЪЕКЦИЙ

Аннотация. Рассматриваются аппаратно-программные и организационные средства защиты ресурсов информационной системы персональных данных от несанкционированного доступа путем SQL-инъекций. В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» под информационной системой персональных данных (далее – ИСПДн) будем понимать совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Анализ безопасности ресурсов ИСПДн относительно несанкционированного доступа к данным (далее – НСД) путем SQL-инъекций включает пять условных этапов: сбор информации в ИСПДн, сканирование ИСПДн, получение доступа к ИСПДн, закрепление в ИСПДн, формирование отчета; при этом анализ безопасности всегда сопряжен с НСД.

Для предотвращения НСД от SQL-инъекций предлагаются следующие программно-аппаратные решения, позволяющие минимизировать последствия несанкционированного воздействия на ИСПДн: брандмауэр web-приложений для фильтрации вредоносных данных; регулярные обновления и исправления; минимизация использования привилегий уровня администратора; минимизация открытой информации об архитектуре баз данных (далее – БД) ИСПДн из сообщений об ошибках; непрерывный мониторинг операторов SQL-инъекций из приложений, подключенных к БД.

Ключевые слова: SQL-инъекция, анализ безопасности, безопасность ресурсов, закрепление в системе, информационная система, персональные данные, получение доступа, сбор информации, сканирование, средства защиты ресурсов, формирование отчета, этапы анализа.

A.R. Gazizov

HARDWARE, SOFTWARE AND ORGANIZATIONAL MEANS OF PROTECTING INFORMATION SYSTEM RESOURCES FROM UNAUTHORIZED ACCESS BY SQL INJECTIONS

Abstract. The article discusses hardware, software and organizational means of protecting the resources of the personal data information system from unauthorized access by SQL injections. The use of cloud storage as a place to store information implies a number of In accordance with Federal Law No. 152-FZ of July 27, 2006 "On Personal Data", the personal Data Information System (ISPDn) will be understood as a set of personal data contained in databases and information technologies and technical means that ensure their processing. The analysis of the security of ISPDn resources with respect to NSD by SQL injection includes five conditional stages: collecting information in ISPDn, scanning ISPDn, gaining access to ISPDn, fixing in ISPDn, generating a report; at the same time, security analysis is always associated with unauthorized access to data.

To prevent NSD from SQL injections, the following hardware and software solutions are proposed to minimize the consequences of unauthorized exposure to ISPDn: a firewall of web applications for filtering malicious data; regular updates and corrections; minimizing the use of administrator-level privileges; minimizing open information about the architecture of the ISPDn database from error messages; continuous monitoring of SQL statements-injections from applications connected to the database.

Keywords: SQL injection, security analysis, resource security, securing in the system, information system, personal data, access, information collection, scanning, resource protection tools, report generation, analysis stages.

Газизов Андрей Равильевич
кандидат педагогических наук, доцент, доцент кафедры вычислительных систем и информационной безопасности. Донской государственный технический университет, город Ростов-на-Дону. Сфера научных интересов: методы и системы защиты информации, информационная безопасность (технические науки), теория и методика обучения и воспитания (информатизация образования). Автор 50 опубликованных научных работ.
Электронный адрес: gazandre@yandex.ru

Введение

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» под ИСПДн будем понимать совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [14].

Анализ безопасности ресурсов ИСПДн относительно НСД проводился в организации, осуществляющей торговую деятельность, после получения письменного разрешения руководителя организации на проведение работ по анализу безопасности ресурсов ИСПДн при условии подписания соглашения о неразглашении информации, полученной в результате анализа.

Анализ безопасности ресурсов ИСПДн относительно НСД путем SQL-инъекций необходимо разделить на пять этапов: сбор информации в ИСПДн; сканирование ИСПДн; получение доступа к ИСПДн; закрепление в ИСПДн; формирование отчета.

Этапы анализа безопасности ресурсов ИСПДн

Этап 1. Сбор информации в ИСПДн условно разделен на пассивную и активную фазы с целью получения ее максимального количества относительно исследуемого объекта информатизации. Этап является наиболее важными и максимально трудоемким.

Во время пассивной фазы ИСПДн «не знает» о том, что был начат сбор информации из открытых и общедоступных источников, таких как поисковые системы и базы данных NIC. Базы данных NIC – это ссылка на запись, которая размещена в базе данных той или иной организации, регулирующей деятельность во всемирной паутине [12]. Активная фаза предполагает непосредственное взаимодействие с самой ИСПДн, в том числе сканирование портов, определение работающих сервисов и их версий, а также определение версий операционной системы, под управлением которой работают конечные пользователи и сервисы.

Этап 2. Сканирование ИСПДн осуществляется на основе информации, полученной на предыдущем этапе, с использованием следующего инструментария: ICMP-сканеры, SNMP-сканеры, сканеры открытых портов, сканеры уязвимостей.

Сканирование ИСПДн позволяет получать следующую информацию: IP-адреса, версии операционных систем, запущенные сервисы и их версии, «имена» компьютеров, учетные записи пользователей.

Этап 3. Получение доступа к ИСПДн. Используя данные, полученные после сканирования ИСПДн, выявляется уязвимость персональных данных.

Этап 4. Закрепление в ИСПДн предполагает закрепление в системе, к которой ранее был получен доступ; это так называемые методы сохранения доступа к ИСПДн – установка троянских программ, backdoor или rootkit.

Этап 5. Формирование отчета.

Подводя итог, следует отметить, что анализ безопасности ресурсов ИСПДн всегда сопряжен с НСД; вопрос состоит исключительно в легитимности мероприятий анализа или ее отсутствии [12].

Анализ безопасности ресурсов ИСПДн путем SQL-инъекций

SQL-инъекция представляет собой несанкционированный доступ к информационным системам, используемым для функционирования поименованной целостной совокупности данных, и отображает состояние объектов и их отношений в ИСПДн. НСД в данном случае представляет собой внедрение кода в существующий запрос с целью получения доступа к ресурсам (данным) ИСПДн и манипулированию ими. Атаки на ИСПДн путем SQL-инъекций осуществляются практически на всех известных платформах [3; 4].

При анализе безопасности ресурсов ИСПДн путем SQL-инъекций изначально необходимо понимать, с какой системой управления базами данных (далее – СУБД) предстоит работать, например, с Oracle Database или Microsoft SQL Server.

В примере ниже дано описание применения кода после символа «;», обозначающего конец запроса:

- SELECT * FROM articles
- WHERE creator = 'bob'
- AND article_name = 'sql_abc';
- DELETEFRO Marticles.

Две вышеуказанные совокупности программных средств (Oracle и Microsoft) обеспечивают возможность создания системы управления базами данных для доступа к данным и управления БД, позволяют выполнить подряд несколько запросов, разделенных символом «;» и следующих друг за другом. Все остальные СУБД завершат процесс с сообщением об ошибке.

В практике функционирования ИСПДн серверы БД и веб-приложений принято разделять. Реализация поиска СУБД определенного типа используется с помощью Nmap (Network Mapper) – утилиты с открытым исходным кодом для исследования сети и проверки безопасности, разработанной для быстрого сканирования больших сетей и единичных целей.

Практическая часть анализа безопасности ресурсов ИСПДн путем SQL-инъекций предполагает применение следующих программных, программно-аппаратных и технических средств и устройств.

1. Персональный компьютер с установленной операционной системой Windows 10, версия сборки 1903.

2. Программное обеспечение Virtual Box. Данная программа эмулирует программное обеспечение компьютера, то есть это виртуальный компьютер, на который установлена операционная система и сопутствующее программное обеспечение. Виртуальный компьютер создает изолированное окружение на компьютере, которое состоит из виртуальных компонентов реального персонального компьютера – жесткий диск, видеокарта, оперативная память, модуль беспроводного соединения Wi-Fi и различные контроллеры устройств [1].

3. Дистрибутив Kali Linux, который имеет большое количество предустановленных программ для тестирования и проникновения, в том числе Armitage (графический инструмент управления кибератакой), nmap (сканер портов), Wireshark (анализатор трафика), взломщик паролей Johnthe Ripper, Aircrack-ng (программный пакет для тестирова-

ния беспроводных локальных сетей), Burp Suite и сканер безопасности веб-приложений OWASPZAP. Дистрибутив Kali Linux будет установлен и сможет работать на виртуальном компьютере [6; 7].

4. Инструментарий sqlmap с открытым исходным кодом для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатации уязвимости SQL-инъекции и захват серверов БД. Инструмент sqlmap имеет широкий набор возможностей – от сбора отпечатков БД по полученной от них информации до доступа к файловой системе и выполнению команд в операционной системе посредством внеполосных (out-of-band) подключений [9].

Использование дистрибутива Kali Linux и инструментария sqlmap обеспечит проведение анализа на наличие возможных уязвимостей web-приложения ИСПДн, где находиться БД с последующим получением полного доступа к ней [6; 7].

Детали анализа

1. Выполняемое действие называется SQL-инъекцией. Для анализа используются дорки – список определенных запросов в поисковой системе, применяемых в процессе выкачивания с сервера баз сайтов с последующим процессом дампа. Под дампом понимается получение несанкционированного доступа и кражи БД с сайта, у которого имеется SQL-уязвимость (SQL-Injection).

2. С помощью программы Gr3Nox (сканера эксплоитов) и выбранного дорка (из списка) выполняется сканирование по выявлению уязвимостей в случайном порядке или определенного web-ресурса. В ходе выполнения анализа был выбран конкретный ресурс ИСПДн рассматриваемой организации и прописан в поля программы, изображенной на Рисунке 1.

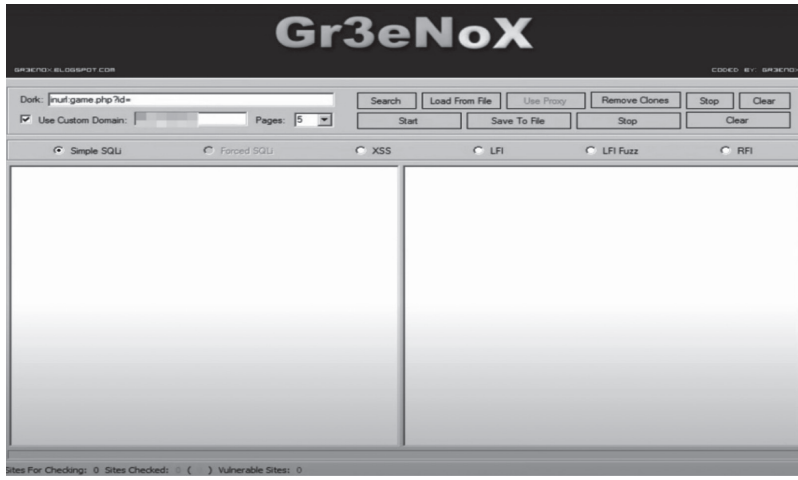

Рисунок 1. Ввод данных в программу

3. Выполняется запуск программы на сканирование и определение уязвимостей. Данный процесс изображен на Рисунке 2. С помощью полученной информации заранее можно сделать вывод о том, что у сайта организации имеется уязвимость, по которой при правильном ее использовании можно получить доступ к БД ИСПДн. Далее анализ проводится в терминале дистрибутива Kali Linux.

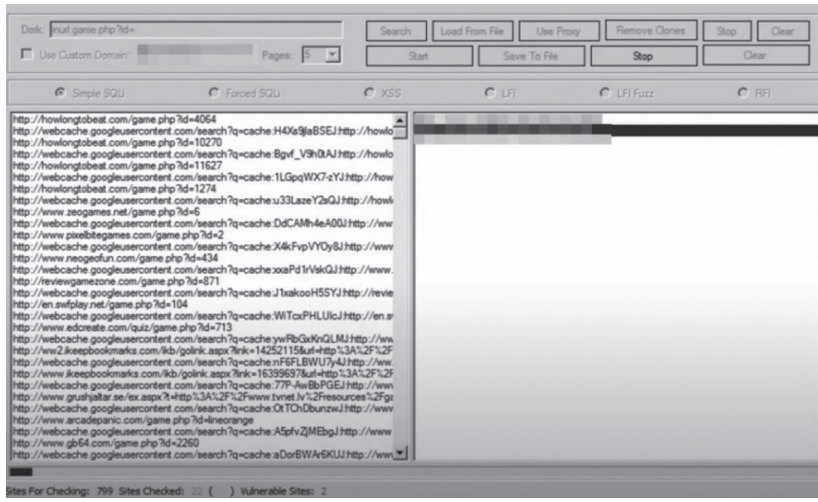

Рисунок 2. Получение результатов сканирования

4. В терминале прописывается следующая команда sqlmap – u (выбранный web-ресурс глобальной сети Интернет) – dbs. После введения команды идет процесс создания директории, после предоставляется один из вариантов для дальнейшего продолжения анализа – continue, string, regex или quit.

Для целей анализа безопасности ресурсов ИСПДн выбираем вариант continue продолжения анализа для получения доступа к БД.

5. Поступает запрос на выполнение команды анализа безопасности ресурсов ИСПДн по всем возможным тестам, в том числе по определенному идентификатору. Для анализа выбираем тест по полученному ранее идентификатору. После завершения сканирования будет получен доступ к трем разделам БД ИС организации, где присутствует различная информация о web-ресурсе. Информация о выполнении анализа представлена на Рисунке 3.

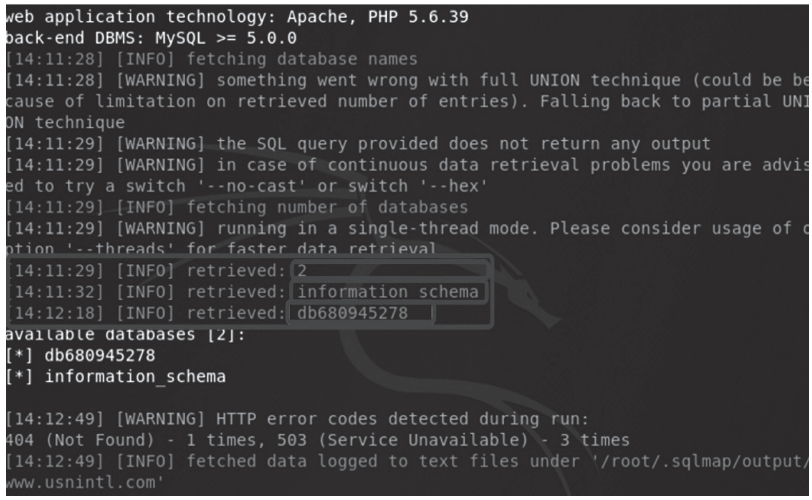

Рисунок 3. Выявленные в процессе сканирования разделы БД

6. Анализ проводится в разделе таблицы (db680945278), в которой могут быть размещены персональные данные сотрудников и клиентов организации. Результат выбора изображен на Рисунке 4.

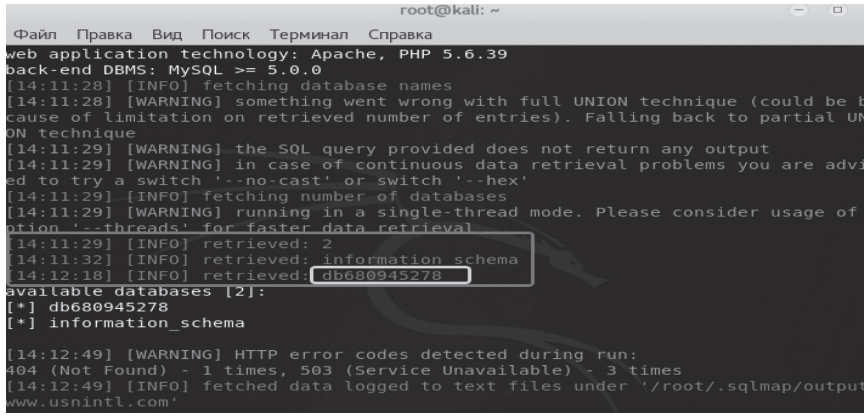

Рисунок 4. Выбор раздела таблицы

7. После выбора таблицы в терминале прописывается следующая команда sqlmap – u (сайт организации) targeturl – Dinformation_schema – tables, чтобы определить наличие вложенных таблиц с данными.

После сканирования на наличие доступных для анализа таблиц наблюдается следующее содержимое, состоящее из девятнадцати таблиц (см. Рисунок 5).

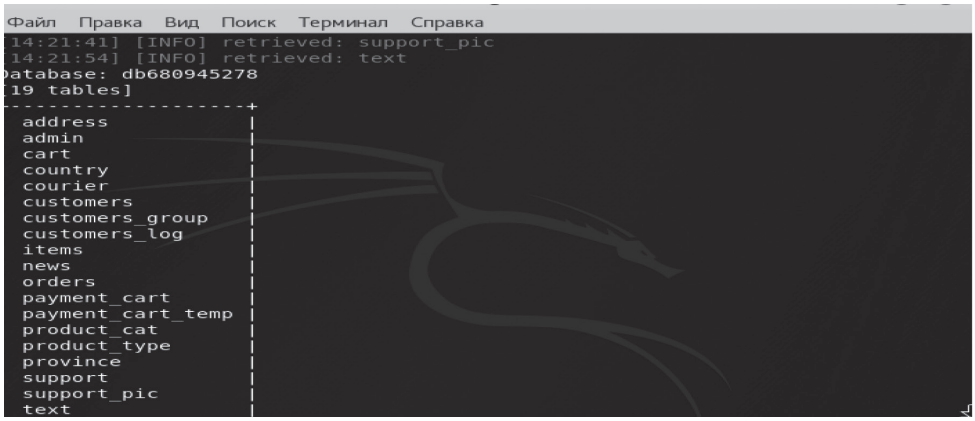

Рисунок 5. Выявленные таблицы

8. Для дальнейшего анализа на проникновение в базу данных web-ресурса рассматриваемой организации определяются таблицы, которые требуют особого внимания: admin, customers.

9. В ходе анализа был получен доступ к таблице admin, данные для получения прав администрирования web-ресурса, представленные на Рисунке 6. После выявления уязвимости данные для идентификации и аутентификации были одномоментно изменены (на рисунке показаны данные до проведения анализа).

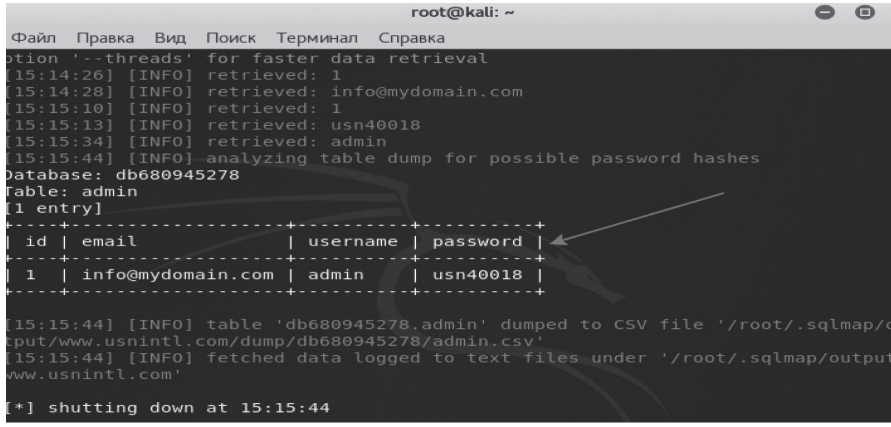

Рисунок 6. Данные для администрирования web-ресурсом

Таким образом, стало возможным получение следующих персональных данных: почта клиента для авторизации на web-ресурсе; пароль; город проживания; номера мобильных телефонов; данные банковских карт; статус клиента (см. Рисунок 7).

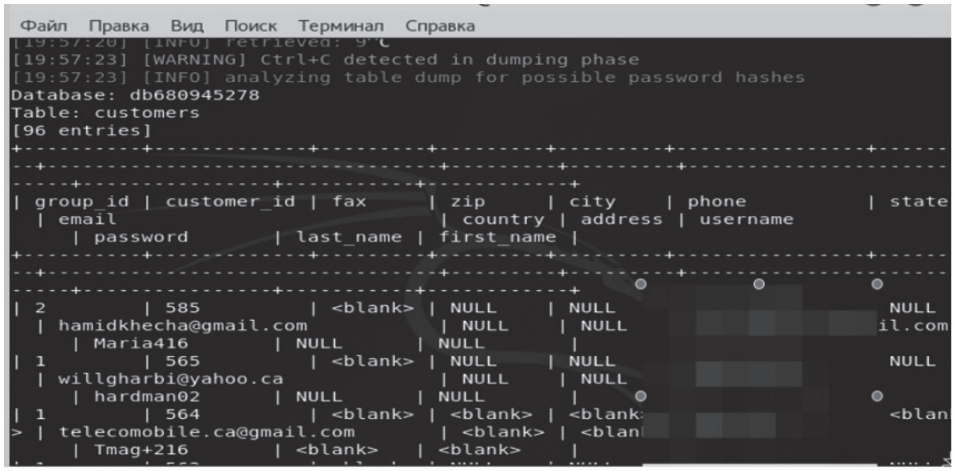

Рисунок 7. Данные клиентов ИСПДн

Исходя из этого можно сделать вывод, что злоумышленник может получить НСД к ресурсам ИСПДн путем SQL-инъекций, в том числе к персональным данным пользователей, действовать от их имени, применять и оплачивать услуги, а также получить полный доступ к web-ресурсу на правах администратора, тем самым навредив организации и ее клиентам.

Заключение

Для предотвращения НСД от SQL-инъекций предлагаются следующие решения (аппаратно-программные и организационные средства защиты ресурсов), позволяющие минимизировать последствия несанкционированного воздействия на ИСПДн.

1. Брандмауэр web-приложений (WAF) – аппаратно-программный фильтр вредоносных данных. Примером является бесплатный модуль с открытым исходным кодом Mod Security, доступный для web-сервисов Apache, Microsoft IIS и nginx. ModSecirity представ-

ляет собой сложный и постоянно развивающийся набор правил для фильтрации потенциально опасных web-запросов. Средства защиты от SQL-инъекций модуля Mod Security могут идентифицировать большинство попыток проникновения SQL через web-каналы.

2. Обновление и исправление. Уязвимости в приложениях и БД ИСПДн, которыми злоумышленники могут воспользоваться с помощью SQL-инъекции, регулярно обнаруживаются, поэтому крайне важно постоянно применять исправления и обновления. Решение по управлению обновлениями предполагает инвестиции.

3. Привилегии уровня администратора с применением учетной записи. Использование учетной записи с ограниченным доступом повысит безопасность и ограничит возможности злоумышленника. Например, код страницы входа в ИСПДн должен запрашивать БД, используя учетную запись, ограниченную соответствующей таблицей учетных данных. Таким образом, НСД через этот канал не может быть реализован для взлома всей БД.

4. Минимизация открытой информации. Злоумышленники могут многое узнать об архитектуре БД ИСПДн из сообщений об ошибках, поэтому необходимо убедиться, что отображается минимальная информация. Следует использовать режим custom Errors и Remote Only, то есть эквивалентный, для отображения подробных сообщений об ошибках на локальном компьютере, гарантирующий, что внешний злоумышленник не получит ничего, кроме сообщения, что его действия привели к необработанной ошибке [5].

5. Непрерывный мониторинг операторов SQL-инъекций из приложений, подключенных к БД, поможет выявить мошеннические операторы SQL-инъекций и их уязвимости; в связи с этим инструменты непрерывного мониторинга, использующие машинное обучение или поведенческий анализ, могут быть особенно полезными.

Литература

1. Geekkies [Электронный ресурс]. URL: https://geekkies.in.ua/crossplatform/chto-takoe-virtualbox-i-kak-ej-polzovatsja.html (дата обращения: 25.06.2022).
2. RU-center [Электронный ресурс]. URL: https://www.nic.ru/help/bazy-dannyh-1228/ (дата обращения: 25.06.2022).
3. Академик – информационная безопасность [Электронный ресурс]. URL: https://dic.academic.ru/dic.nsf/dic_economic_law/5569/ИНФОРМАЦИОННАЯ (дата обращения: 25.06.2022).
4. Академик – официальная терминология [Электронный ресурс]. URL: https://official.academic.ru/7175 (дата обращения: 25.06.2022).
5. Академик – словарь чрезвычайных ситуаций [Электронный ресурс]. URL: https://dic.academic.ru/dic.nsf/emergency/777/ (дата обращения: 25.06.2022).
6. Kali Linux // Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Kali_Linux (дата обращения: 25.06.2022).
7. Инструменты Kali Linux [Электронный ресурс]. URL: https://kali.tools/?p=816 (дата обращения: 25.06.2022).
8. Об информации, информационных технологиях и о защите информации: ФЗ от 27.07.2006 № 149-ФЗ / Консультант плюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 25.06.2022).
9. Основные проблемы защиты информации в сетях [Электронный ресурс]. URL: https://zen.yandex.com/media/id/5da8242eaad43600b1f1f9ed/osnovnye-problemy-zascity-informacii-v-setiah-5da82678c31e4900ae31ec07 (дата обращения: 25.06.2022).

10. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119 [Электронный ресурс]. URL: http://government.ru/docs/all/84743/ (дата обращения: 25.06.2022).
11. Сдам сам: Выбор и обоснование методики расчета экономической эффективности [Электронный ресурс]. URL: http://zdamsam.ru (дата обращения: 25.06.2022).
12. *Скабцов Н.* Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.: ил. (Серия «Библиотека программиста»).
13. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18 февраля 2013 г. N 21 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 25.06.2022).
14. О персональных данных: ФЗ от 27.07.2006 N 152-ФЗ [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/365-federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz?highlight=WyIxNTItXHUwNDQ0XHUwNDM3Il0= (дата обращения: 25.06.2022).

References

1. Geekkies. Available at: https://geekkies.in.ua/crossplatform/chto-takoe-virtualbox-i-kak-ej-polzovatsja.html (date of the application: 25.06.2022).
2. RU-center. Available at: https://www.nic.ru/help/bazy-dannyh-1228 (date of the application: 25.06.2022).
3. *Akademik – informatsionnaya bezopasnost'* [Academician – information security]. Available at: https://dic.academic.ru/dic.nsf/dic_economic_law/5569/ИНФОРМАЦИОННАЯ (date of the application: 25.06.2022) (in Russian).
4. *Akademik – ofitsial'naya terminologiya* [Academician – official terminology]. Available at: https://official.academic.ru/7175 (date of the application: 25.06.2022) (in Russian).
5. *Akademik – slovar' chrezvychainykh situatsii* [Academician – Dictionary of Emergency Situations]. Available at: https://dic.academic.ru/dic.nsf/emergency/777 (date of the application: 25.06.2022) (in Russian).
6. Kali Linux // Wikipedia. Available at: https://ru.wikipedia.org/wiki/Kali_Linux (date of the application: 25.06.2022) (in Russian).
7. *Instrumenty Kali Linux* [Kali Linux Tools]. Available at: https://kali.tools/?p=816 (date of application: 25.06.2022) (in Russian).
8. *Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: FZ ot 27.07.2006 N 149-FZ* [About information, information technologies and information protection: Federal Law No. 149-FZ of 27.07.2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61798 (date of the application: 25.06.2022) (in Russian).
9. *Osnovnye problemy zashchity informatsii v setyakh* [The main problems of information protection in networks]. Available at: https://zen.yandex.com/media/id/5da8242eaad43600b1f1f9ed/osnovnye-problemy-zascity-informacii-v-setiah-5da82678c31e4900ae31ec07 (date of application: 25.06.2022) (in Russian).
10. *Ob utverzhdenii trebovanii k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Postanovlenie Pravitel'stva RF ot 01.11.2012 № 1119* [On approval of

the requirements for the protection of personal data during their processing in personal data information systems: Decree of the Government of the Russian Federation No. 1119 of 01.11.2012. Available at: http://government.ru/docs/all/84743 (date of the application: 25.06.2022) (in Russian).
11. *Sdam sam: Vybor i obosnovanie metodiki rascheta ekonomicheskoi effektivnosti* [I will take it myself: The choice and justification of the methodology for calculating economic efficiency]. Available at: http://zdamsam.ru (date of the application: 25.06.2022) (in Russian).
12. Skabtsov N. (2018) *Audit bezopasnosti informatsionnykh sistem* [Information systems security audit]. St. Petersburg, Piter Publishing, 272 p. (in Russian).
13. *Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh, pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Prikaz FSTEK Rossii ot 18 fevralya 2013 g. N 21* [On the approval of the composition and content of organizational and technical measures to ensure, the security of personal data when they are processed in personal data information systems: Order of the FSTEC of Russia dated February 18, 2013 N 21]. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (date of the application:25.06.2022) (in Russian).
14. *O personal'nykh dannykh: FZ ot 27.07.2006 N 152-FZ* [About personal data: Federal Law No. 152-FZ of 27.07.2006. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/365-federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz?highlight=WyIxNTItXHUwNDQ0XHUwNDM3Il0 = (date of the application: 25.06.2022) (in Russian).