УДК 004.056+004.45 **DOI 10.25799/AR.2019.80.1.006**

Особенности функционирования криптологического программного комплекса «креветка»

Быстрицкий Николай Дмитриевич

Кандидат технических наук,
младший научный сотрудник,
научно-исследовательский вычислительный центр,
Московский государственный университет им. М.В. Ломоносова,
119234, Российская Федерация, Москва, Ленинские Горы, 1;
e-mail: fastnika@yandex.ru

Макаров-Землянский Николай Викулович

Доктор технических наук, кандидат физико-математических наук,
ведущий научный сотрудник,
научно-исследовательский вычислительный центр,
Московский государственный университет им. М.В. Ломоносова,
119234, Российская Федерация, Москва, Ленинские Горы, 1;
e-mail: nvmz@yandex.ru

Назаров Владимир Сергеевич

Студент 5-го курса,
научно-исследовательский вычислительный центр,
Московский государственный университет им. М.В. Ломоносова,
119234, Российская Федерация, Москва, Ленинские Горы, 1;
e-mail: vovik_n@mail.r

Аннотация

Целью данной статьи является описание особенностей функционирования криптологического программного комплекса поиска источника несанкционированного распространения документов «Креветка». В статье рассмотрены вопросы последовательного внедрения программного комплекса с учетом особенностей структуры организации, а также описаны технологические процессы при его настройке и последующей эксплуатации.

Целью исследования является противодействие утечкам информации в электронно-бумажном документообороте при передаче информации ограниченного доступа, которое предполагает решение как административных, так и практических вопросов. Задачами исследования являются не только предотвращение кражи в сфере информационной безопасности, но и своевременное выявление источника утечки - важно определить потенциального виновника или злоумышленника. Гипотеза исследования представляется тем, что с целью решения поставленной задачи в статье описан алгоритм работы криптологического программного комплекса поиска источника несанкционированного

распространения документов «Креветка». Использованы преимущественно спектрографические и инструментальные методы исследования. В качестве результатов исследования можно отметить следующее. Стремительное развитие компьютерных технологий в конце XX - начале XXI вв. дало человечеству не только возможность автоматизации вычислительных процессов, обмена и хранения информации, но и сформировало новую культуру мышления. Такие достоинства, как возможность межпользовательского взаимодействия данными, удаленная работа и простота использования позволили стремительно проникнуть информатизации во все сферы жизни и повысить эффективность предоставления услуг. Для идентификации источника утечки информации в системе электронного документооборота ограниченного доступа в графическом или текстовом виде был разработан криптологический программный комплекс «Креветка».

Для цитирования в научных исследованиях

Быстрицкий Н.Д., Макаров-Землянский Н.В., Назаров В.С. Особенности функционирования криптологического программного комплекса «креветка» // Экономика: вчера, сегодня, завтра. 2019. Том 9. № 1А. С. 51-60.

Ключевые слова

безопасность, документооборот, противодействие утечкам, поиск инсайдера.

Введение

Сегодня, хищение электронных и печатных документов ограниченного распространения является одной из главных угроз безопасности, которая может нанести существенный вред деятельности организации. Предотвращение таких действий возможно при внедрении специализированных программных средств на автоматизированные рабочие места сотрудников, которые непосредственно участвуют в электронно-бумажном документообороте организации. Помимо использования специальных архитектурных и технологических решений в применяемом программном обеспечении, в большинстве случаев также требуются дополнительные организационно-технические меры. Для минимизации вносимых изменений в установленный регламент работы организации при внедрении криптологического программного комплекса источника несанкционированного распространения документов (КПК ИНРД) «Креветка» [Быстрицкий, 2018, 14] необходимы следующие условия:

- наличие установленного (сформированного) программного обеспечения, непосредственно участвующего в электронно-бумажном документообороте для взаимодействия с КПК ИНРД «Креветка»;
- наличие оборудования, удовлетворяющего минимальным техническим требованиям для функционирования КПК ИНРД «Креветка»;
- организация подготовки сотрудников для выполнения новых должностных обязанностей в соответствии с разработанным дополнением к регламенту работы организации.

Материалы и методы

Выполнение первого требования предполагает использование совместимого с КПК ИНРД «Креветка» программного обеспечения (для государственных структур – рекомендуемого

Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации [Единый реестр]) следующего состава (типа):

- операционной системы (ОС);
- пакета офисных приложений для создания и редактирования документов;
- средства криптографической защиты информации (СКЗИ) для шифрования файлов и формирования электронной подписи в соответствии с отечественными стандартами ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012), ГОСТ 28147-89, а также требованиями Федерального закона РФ от 6 апреля 2011г. №63-ФЗ «Об электронной подписи»;
- программного решения, реализующего функции СКЗИ, поддерживающего работу с различными типами носителей ключевой информации и имеющего поддержку сертификатов ключей, списков отозванных сертификатов в соответствии со стандартами RFC X.509, RFC 4491, RFC 2314;
- программного решения для работы с различными популярными форматами сжатия данных и подготовки документов адресата в виде единого архива или (в зависимости от пропускной способности канала) списка частей архива [Bangerte, 2010, 300];
- отдельного программного решения для работы с шифрованной почтовой корреспонденцией в соответствии с реализованными функциями СКЗИ и стандартами RFC 4490 и RFC 4357, поддерживающего автоматизированную конвертацию файлов адресатов в виде отдельных писем.

Помимо этого, также необходима информация об иерархической структуре подразделений, непосредственно участвующих в пересылке документов ограниченного распространения, представленная в виде базы данных с указанием их кодового мнемонического обозначения и электронного почтового адреса [Brandt, 2001, 158].

Для функционирования КПК ИНРД «Креветка» аппаратная составляющая должна содержать:

- персонализированные устройства, предназначенные для идентификации пользователя (например, USB-ключ или смарт-карта);
- учтенные машинные носители, участвующие в электронном документообороте при разработке печатной версии документа;
- персонализированный (персонифицированный) компьютер, обладающий необходимым быстродействием для автоматизированной обработки документов за ограниченное время с выделенными правами пользователя для осуществления операций [Devanbu, 1997, 401].

Наличие вышеперечисленных аппаратно-программных требований является необходимым условием для работы с КПК ИНРД «Креветка». Достаточным же условием является назначение сотрудников из штата организации, ответственных за КПК ИНРД «Креветка», и наделение их полномочиями для организации электронно-бумажного документооборота. Квалификация данных сотрудников, с одной стороны, должна позволять им участвовать в автоматизированной работе с документами для отправки почтовой корреспонденции, и с другой – обеспечивать поддержание в работоспособном состоянии программного комплекса (в т.ч. при внештатных ситуациях) исходя из установленного регламента работы и личного опыта [Imai, 2011, 287].

Важно также отметить, что КПК ИНРД «Креветка» обеспечивает только автоматизацию процессов электронно-бумажного документооборота и не контролирует саму организацию разработки исполнителем задействованного в отправке почтовой корреспонденции документа. Назначение и функциональные особенности разработанного программного комплекса подразумевает

установленный режим конфиденциальности при работе с информацией ограниченного доступа, при котором исполнитель производит обработку, модификацию и распространение информации в соответствии с установленным регламентом организации [Mao, 1997, 12]. Более того, архитектурные особенности программного комплекса позволяют разграничить функциональные обязанности сотрудника в зависимости от его непосредственного участия в организации электронно-бумажного документооборота. Такое разделение обязанностей предполагает четкое определение функциональных задач для каждого сотрудника подразделения. Их совмещение теряет главное достоинство программного комплекса – его масштабируемость. Поэтому, в случае отсутствия в организации разграничения функциональных обязанностей сотрудников для эффективного применения программного комплекса необходимо провести дополнительные исследования особенностей структуры организации совместно с разработчиками и сформировать наиболее приемлемое архитектурное решение для его внедрения [Minier, 2012, 80].

Первоначальный этап установки КПК ИНРД «Креветка» подразумевает формирование Отделом информационной безопасности организации типовых настроек уникальных параметров программного комплекса в соответствии с утвержденной политикой в части стеганографии. И хотя в КПК ИНРД «Креветка» существуют штатные настройки (настройки по умолчанию), однако они используются только для демонстрации его функциональных возможностей. Формирование таких настроек в виде переносимого администратором безопасности файла может стать угрозой безопасности организации в случае предоставления этой информации третьим лицам [Moldovyan, 1993, 664]. Тем не менее:

- данные настройки могут быть сформированы индивидуально для каждого сотрудника и быть легко скорректированы при установке на конкретное локальное рабочее место, поэтому типовые настройки, сформированные администратором безопасности, могут лишь служить для формирования рекомендуемой политики информационной безопасности подразделения предприятия;

- переносимые настройки программного комплекса, созданные администратором безопасности, могут быть зашифрованы администратором безопасности личным ключом, поэтому в случае утечки такой информации третьим лицам воспользоваться ей окажется весьма затруднительно.

Предварительный этап установки КПК ИНРД «Креветка» на рабочее место сотрудника заключается в проверке наличия совместимого программного обеспечения и оборудования. На данном этапе также происходит формирование исходных данных и на их основе оценка возможности установки программного комплекса на конкретное локальное рабочее место [Nurmi, 1994, 320]. В случае возникновения неполадок, программный комплекс автоматически формирует перечень рекомендаций для их устранения.

Дальнейшая установка КПК ИНРД «Креветка» заключается не только в размещении файлов в директориях на пользовательском компьютере, но и в применении к предустановленному программному комплексу ранее сформированных Отделом информационной безопасности организации настроек. Дополнительному конфигурированию также подлежит указание положения подразделения пользователя в иерархической структуре, используемого локального профиля (надстройки) для работы с носителем ключевой информации, ассоциированной директории с программным решением для работы с шифрованной почтовой корреспонденцией [Schartner, 2010, 182]. Несмотря на кажущуюся сложность проведения установки, весь процесс не занимает много времени при наличии совместимого оборудования и программного обеспечения.

Результаты и обсуждение

Технологический процесс использования КПК ИНРД «Креветка» состоит в автоматизированной передаче документа в подразделения организации в соответствии со списком адресатов рассылки и локализации источника утечки информации из подразделений при обнаружении его в открытом доступе. Этот процесс состоит из следующих этапов:

1. Документ, подготовленный исполнителем или группой исполнителей, проходит этап согласования с руководителем подразделения. В окончательной редакции, документ передается ответственному работнику со списком адресатов для рассылки;

2. Ответственный работник подписывает согласованный документ в двух вариантах – бумажном и электронном. В бумажном варианте на документ ставится подпись руководителя подразделения, в электронном варианте документа с помощью программного комплекса формируется электронная подпись (ЭП). После проведения данных процедур ответственный работник подразделения передает документы сотруднику Отдела почтовой корреспонденции;

3. Сотрудник Отдела почтовой корреспонденции выполняет автоматизированную обработку документов с помощью КПК ИНРД «Креветка» и отправляет их адресатам согласно сформированному ранее списку рассылки.

Стоит отметить, что наибольшую ценность документ представляет именно на финальной стадии готовности, т.к. имеет наибольшую информативность (утвержден и подготовлен к рассылке [Suriadi, 2012, 261]). Поэтому для злоумышленника документ представляет наибольший интерес только с момента его передачи для дальнейшей обработки от исполнителя к другим сотрудникам подразделения. Однако, утечку информации в этом случае возможно решить только административными мерами ввиду того, что документ может быть передан, скопирован и отредактирован различными способами и средствами, в том числе и исполнителем при подготовке документа могут быть использованы различные программные решения, которые индивидуальны при разработке каждого документа [Thorpe,2009,300]. Тем не менее, при передаче документа, адресату попадет только стеганографированнный документ, который не теряет уже свои свойства при дальнейшей передаче на следующем цикле обработки, тем самым утечка документа от адресата на одной из цепочек передачи по одному из каналов данных предопределяет проведение служебной проверки в отношении руководителя этого подразделения. Это обусловлено тем, что при каждой итерации передачи документа администратор безопасности обладает достаточной информацией, чтобы автоматизированными средствами определить источник утечки.

Рассмотрим более детально каждый из представленных вариантов и выявим отличия в передаче, стеганографировании и выявлении источника утечки документа. На Рис. 1 представлено взаимодействие подразделений при разработке документа для внутреннего документооборота [Vorobyev, 2019, 688]. В каждом из представленных подразделений используется КПК ИНРД «Креветка». Отметим, что для «Подразделения 3» и хотя указан только «АРМ Отправки документа», сотрудники с другими функциональными обязанностями также работают в этом подразделении, но не участвуют в представленных взаимодействиях.

На Рис. 1 рассмотрены два случая:

1. Разработанный исполнителем «Подразделения 1» документ передается в «Подразделение 2». На базе полученного документа «Подразделение 2» изготавливает собственный вариант данного документа и пересылает в «Подразделение 3». Такой вариант

считается типичным, например, при разработке общих неконкретизированных рекомендаций, где в «Подразделении 2» производят их уточнение и доводят до «Подразделения 3».

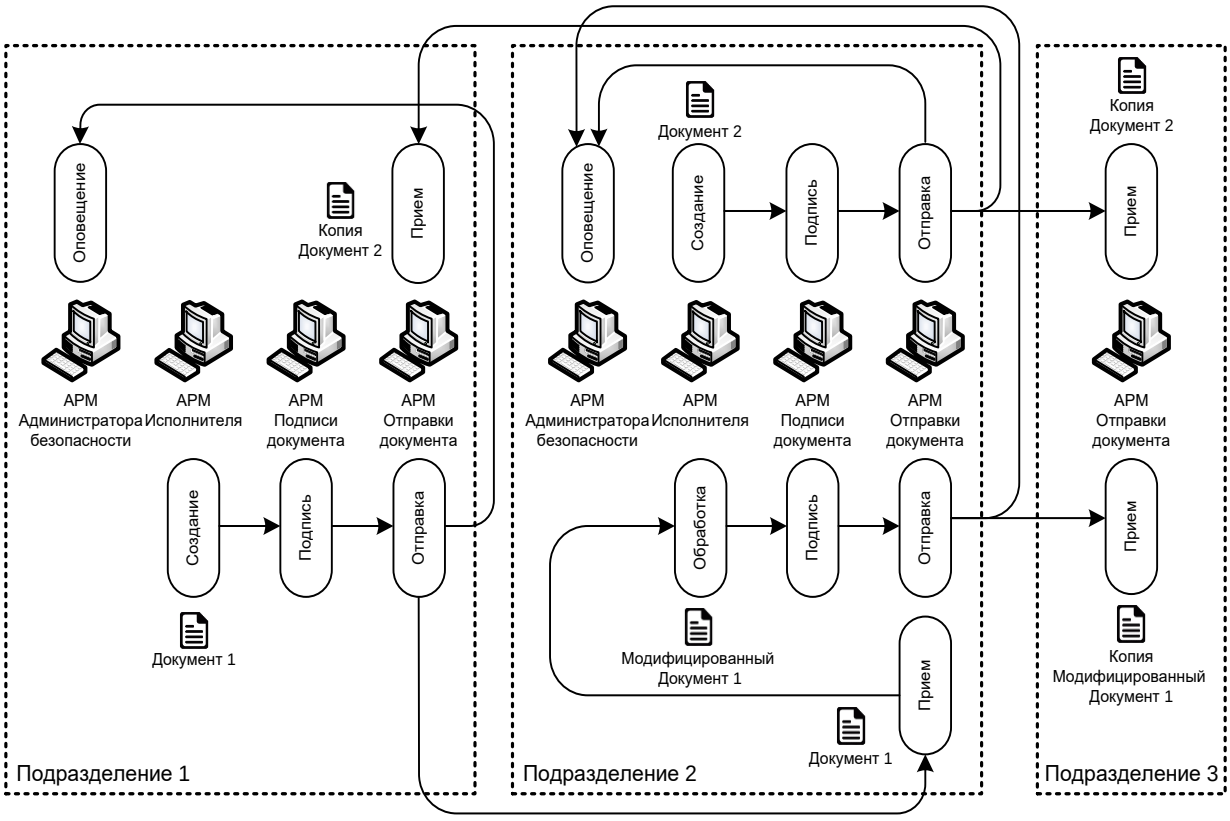

Рисунок 1 – Пример типового электронно-бумажного документооборота организации с использованием КПК ИНРД «Креветка»

2. Разработанный исполнителем «Подразделения 2» документ передается веерной рассылкой в «Подразделение 1» и «Подразделение 3». Такой вариант считается наиболее типичным при обмене информацией между подразделениями и возможен, например, при формировании за определенный период накопленной информации в виде методики, которая передается в другие подразделения для её согласования. В этом случае, каждое из подразделений получает копию разработанного «Подразделением 2» документа. Причем, при использовании КПК ИНРД «Креветка» каждое из подразделений получает не просто дубликат экземпляра документа, а собственный уникальный экземпляр, который визуально отличим только для администратора безопасности [Zhang, 2017, 549].

В отличие от второго варианта, первый вариант передачи подразумевает доработку «Подразделением 2» переданного документа. И хотя модификация такого документа подразумевает нарушение структуры стеганографированного документа, изменение всего документа все же зависит от сконфигурированных Отделом информационной безопасности настроек для КПК ИНРД «Креветка». Таким образом, переданный документ может быть определен администратором безопасности «Подразделения 1» как уникальный, но более важно, что он также будет определен как уникальный для администратора безопасности «Подразделения 2». Тем не менее, важен тот факт, что в случае утечки документа в

«Подразделении 2», это не останется незамеченным для администратора безопасности «Подразделения 1».

Заключение

Рассмотренные оба варианта показывают, что для более эффективного поиска источника утечки похищенного документа необходимо постоянное взаимодействие администраторов безопасности «Подразделения 1» и «Подразделения 2». И хотя это на Рис. 1 не указано, подразумевается, что проводится постоянная синхронизация накопленной статистики между Отделами информационной безопасности «Подразделения 1» и «Подразделения 2». Это позволяет автоматизировать процесс проведения расследований инцидентов в штатном режиме работы КПК ИНРД «Креветка» без создания координационной комиссии. Тем не менее, даже в случае автономной работы каждого из Отделов информационной безопасности, их эффективность не снизится, однако в этом случае ответственность администратора безопасности будет определяться только локально для каждого из подразделений.

Библиография

1. Быстрицкий Н.Д., Макаров-Землянский Н.В., Матвеева Т.В. Криптологический программный комплекс поиска источника несанкционированного распространения документов «Креветка» // Перспективы науки. – 2018. – № 7 (106). – 12–15 с.
2. Единый реестр российских программ для электронных вычислительных машин и баз данных [Официальный сайт]. URL: https://reestr.minsvyaz.ru/
3. Bangerter, E et al. 2010. “Using Compilers to Enhance Cryptographic Product Development.” In ISSE 2009 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2009 Conference, eds. Norbert Pohlmann, Helmut Reimer, and Wolfgang Schneider. Wiesbaden: Vieweg+Teubner, 291–301. https://doi.org/10.1007/978-3-8348-9363-5_29.
4. Brandt, Felix. 2001. “Cryptographic Protocols for Secure Second-Price Auctions.” In Cooperative Information Agents V, eds. Matthias Klusch and Franco Zambonelli. Berlin, Heidelberg: Springer Berlin Heidelberg, 154–65.
5. Devanbu, Prem, and Stuart G Stubblebine. 1997. “Cryptographic Verification of Test Coverage Claims.” In Software Engineering --- ESEC/FSE’97, eds. Mehdi Jazayeri and Helmut Schauer. Berlin, Heidelberg: Springer Berlin Heidelberg, 395–413.
6. Imai, Hideki, and Atsuhiro Yamagishi. 2011. “CRYPTREC (Japanese Cryptographic Algorithm Evaluation Project).” In Encyclopedia of Cryptography and Security, eds. Henk C A van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 285–88. https://doi.org/10.1007/978-1-4419-5906-5_567.
7. Mao, Wenbo. 1997. “On Cryptographic Techniques for On-Line Bankcard Payment Transactions Using Open Networks.” In Security Protocols, ed. Mark Lomas. Berlin, Heidelberg: Springer Berlin Heidelberg, 1–17.
8. Minier, Marine, and Raphael C -W. Phan. 2012. “Energy-Efficient Cryptographic Engineering Paradigm.” In Open Problems in Network Security, eds. Jan Camenisch and Dogan Kesdogan. Berlin, Heidelberg: Springer Berlin Heidelberg, 78–88.
9. Moldovyan, A A, and N A Moldovyan. 1993. “New Design Principle for Cryptographic Modules in Computer Security Systems.” Cybernetics and Systems Analysis 29(5): 663–69. https://doi.org/10.1007/BF01125796.
10. Nurmi, Hannu. 1994. “Cryptographic Protocols for Auctions and Bargaining.” In Results and Trends in Theoretical Computer Science: Colloquium in Honor of Arto Salomaa Graz, Austria, June 10--11, 1994 Proceedings, eds. Juliani Karhumäki, Hermann Maurer, and Grzegorz Rozenberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 317–24. https://doi.org/10.1007/3-540-58131-6_56.
11. Schartner, P, and C Kollmitzer. 2010. “Quantum-Cryptographic Networks from a Prototype to the Citizen.” In Applied Quantum Cryptography, eds. Christian Kollmitzer and Mario Pivk. Berlin, Heidelberg: Springer Berlin Heidelberg, 173–84. https://doi.org/10.1007/978-3-642-04831-9_9.
12. Suriadi, Suriadi, Chun Ouyang, and Ernest Foo. 2012. “Privacy Compliance Verification in Cryptographic Protocols.” In Transactions on Petri Nets and Other Models of Concurrency VI, eds. Kurt Jensen et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 251–76. https://doi.org/10.1007/978-3-642-35179-2_11.
13. Thorpe, Christopher, and David C Parkes. 2009. “Cryptographic Combinatorial Securities Exchanges.” In Financial

Cryptography and Data Security, eds. Roger Dingledine and Philippe Golle. Berlin, Heidelberg: Springer Berlin Heidelberg, 285–304.
14. Vorobyev, Gennady A, Vladimir A Kozlov, and Viktoria A Ryndiuk. 2019. “Peculiarities of Cryptographic Model of the System of Wireless Remote Control.” In Perspectives on the Use of New Information and Communication Technology (ICT) in the Modern Economy, eds. Elena G Popkova and Victoria N Ostrovskaya. Cham: Springer International Publishing, 684–92.
15. Zhang, Ming-qing et al. 2017. “Modeling and Simulation Strategies of Cryptographic Protocols Based on Finite State Machine.” In Information Technology and Intelligent Transportation Systems, eds. Valentina Emilia Balas, Lakhmi C Jain, and Xiangmo Zhao. Cham: Springer International Publishing, 541–51.

Features of functioning of the cryptologic software package "shrimp”

Nikolai D. Bystritskii

PhD in Technical Sciences,
Junior Researcher, Research Computing Center,
Lomonosov Moscow State University,
119234, 1, Leninskie Gory, Moscow, Russian Federation;
e-mail: fastnika@yandex.ru

Nikolai V. Makarov-Zemlyanskii

Doctor of Technical Sciences, PhD in Physical and Mathematical Sciences,
Leading Researcher, Research Computing Center,
Lomonosov Moscow State University,
119234, 1, Leninskie Gory, Moscow, Russian Federation;
e-mail: nvmz@yandex.ru

Vladimir S. Nazarov

5th year student,
Research Computing Center,
Lomonosov Moscow State University,
119234, 1, Leninskie Gory, Moscow, Russian Federation;
e-mail: vovik_n@mail.ru

Annotation

The purpose of this article is to describe the features of the functioning of the cryptological software complex to find the source of unauthorized distribution of documents "shrimp". The article deals with the issues of consistent implementation of the software complex taking into account the structure of the organization, as well as the technological processes in its configuration and subsequent operation.

The aim of the study is to counter the leakage of information in the electronic and paper documents in the transmission of limited access information, which involves the solution of both administrative and practical issues. The objectives of the study are not only to prevent theft in the field of information security, but also the timely identification of the source of the leak - it is

important to identify the potential culprit or attacker. The hypothesis of the study is that in order to solve this problem, the article describes the algorithm of the cryptological software complex to find the source of unauthorized distribution of documents "Shrimp". Mainly spectrographic and instrumental methods of research are used. The results of the study include the following. The rapid development of computer technology in the late XX - early XXI centuries. it gave mankind not only the opportunity to automate computing processes, exchange and storage of information, but also formed a new culture of thinking. Such advantages as the possibility of inter-user interaction with data, remote operation and ease of use have allowed to rapidly penetrate all spheres of life and improve the efficiency of services. To identify the source of information leakage in the electronic document management system of limited access in graphical or textual form, a cryptological software complex "Shrimp" was developed.

For citation

Bystritskii N.D., Makarov-Zemlyanskii N.V., Nazarov V.S. (2019) Podkhody k otsenke ushcherba ot tsenovoy diskriminatsii v antimonopol'nom regulirovanii [Features of functioning of the cryptologic software package "shrimp"]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 9 (1A), pp. 51-60.

Keywords

Security, document management, combating leakages, search for the insider.

References

1. Bystritskiy N.D., Makarov-Zemlyanskiy N.V., Matveyeva T.V. Kriptologicheskiy programmnyy kompleks poiska istochnika nesanktsionirovannogo rasprostraneniya dokumentov «Krevetka» [Cryptological software complex for searching for the source of unauthorized distribution of Shrimp documents]. *Perspektivy nauk*i – *Science Prospects*, 2018, no. 7 (106), pp. 12-15.
2. The Unified Register of Russian Programs for Electronic Computers and Databases [Official Website]. URL: https://reestr.minsvyaz.ru/
3. Bangerter, E et al. 2010. “Using Compilers to Enhance Cryptographic Product Development.” In ISSE 2009 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2009 Conference, eds. Norbert Pohlmann, Helmut Reimer, and Wolfgang Schneider. Wiesbaden: Vieweg+Teubner, 291–301. https://doi.org/10.1007/978-3-8348-9363-5_29.
4. Brandt, Felix. 2001. “Cryptographic Protocols for Secure Second-Price Auctions.” In Cooperative Information Agents V, eds. Matthias Klusch and Franco Zambonelli. Berlin, Heidelberg: Springer Berlin Heidelberg, 154–65.
5. Devanbu, Prem, and Stuart G Stubblebine. 1997. “Cryptographic Verification of Test Coverage Claims.” In Software Engineering --- ESEC/FSE’97, eds. Mehdi Jazayeri and Helmut Schauer. Berlin, Heidelberg: Springer Berlin Heidelberg, 395–413.
6. Imai, Hideki, and Atsuhiro Yamagishi. 2011. “CRYPTREC (Japanese Cryptographic Algorithm Evaluation Project).” In Encyclopedia of Cryptography and Security, eds. Henk C A van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 285–88. https://doi.org/10.1007/978-1-4419-5906-5_567.
7. Mao, Wenbo. 1997. “On Cryptographic Techniques for On-Line Bankcard Payment Transactions Using Open Networks.” In Security Protocols, ed. Mark Lomas. Berlin, Heidelberg: Springer Berlin Heidelberg, 1–17.
8. Minier, Marine, and Raphael C -W. Phan. 2012. “Energy-Efficient Cryptographic Engineering Paradigm.” In Open Problems in Network Security, eds. Jan Camenisch and Dogan Kesdogan. Berlin, Heidelberg: Springer Berlin Heidelberg, 78–88.
9. Moldovyan, A A, and N A Moldovyan. 1993. “New Design Principle for Cryptographic Modules in Computer Security Systems.” Cybernetics and Systems Analysis 29(5): 663–69. https://doi.org/10.1007/BF01125796.
10. Nurmi, Hannu. 1994. “Cryptographic Protocols for Auctions and Bargaining.” In Results and Trends in Theoretical Computer Science: Colloquium in Honor of Arto Salomaa Graz, Austria, June 10--11, 1994 Proceedings, eds. Juliani Karhumäki, Hermann Maurer, and Grzegorz Rozenberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 317–24. https://doi.org/10.1007/3-540-58131-6_56.
11. Schartner, P, and C Kollmitzer. 2010. “Quantum-Cryptographic Networks from a Prototype to the Citizen.” In Applied

Quantum Cryptography, eds. Christian Kollmitzer and Mario Pivk. Berlin, Heidelberg: Springer Berlin Heidelberg, 173–84. https://doi.org/10.1007/978-3-642-04831-9_9.

12. Suriadi, Suriadi, Chun Ouyang, and Ernest Foo. 2012. "Privacy Compliance Verification in Cryptographic Protocols." In Transactions on Petri Nets and Other Models of Concurrency VI, eds. Kurt Jensen et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 251–76. https://doi.org/10.1007/978-3-642-35179-2_11.
13. Thorpe, Christopher, and David C Parkes. 2009. "Cryptographic Combinatorial Securities Exchanges." In Financial Cryptography and Data Security, eds. Roger Dingledine and Philippe Golle. Berlin, Heidelberg: Springer Berlin Heidelberg, 285–304.
14. Vorobyev, Gennady A, Vladimir A Kozlov, and Viktoria A Ryndiuk. 2019. "Peculiarities of Cryptographic Model of the System of Wireless Remote Control." In Perspectives on the Use of New Information and Communication Technology (ICT) in the Modern Economy, eds. Elena G Popkova and Victoria N Ostrovskaya. Cham: Springer International Publishing, 684–92.
15. Zhang, Ming-qing et al. 2017. "Modeling and Simulation Strategies of Cryptographic Protocols Based on Finite State Machine." In Information Technology and Intelligent Transportation Systems, eds. Valentina Emilia Balas, Lakhmi C Jain, and Xiangmo Zhao. Cham: Springer International Publishing, 541–51.