DOI: 10.18137/RNU.V9187.23.04.P.108 УДК 004.056

Х.Т. Каримов, В.А. Андрианов, В.Н. Пермяков, Л.М. Тархова, В.Г. Урманов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ПУТЬ К ЭФФЕКТИВНОСТИ РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. Рассматриваются вопросы, относящиеся к текущему состоянию безопасности компьютерных сетей. Производится анализ факторов, влияющих на безопасность компьютерных сетей. Поднимаются вопросы необходимости усиления безопасности компьютерных сетей и эффективности использования технологий шифрования для безопасности данных.

Ключевые слова: информационная безопасность, кибербезопасность, безопасность сетей.

Kh.T. Karimov, V.A. Andrianov, V.N. Permyakov, L.M. Tarkhova, V.G. Urmanov

INFORMATION SECURITY AS A PATH TO INFORMATION SYSTEMS EFFICIENCY

Abstract. The article addresses the issues related to the current state of computer network security and the need to strengthen its security. An analysis of factors affecting the security of computer networks is carried out. The authors raise the question of the effectiveness of using encryption technology for data security and computer network security.

Keywords: information security, cybersecurity, network security.

Введение

С развитием технологий мобильной связи зависимость электронных компьютеров в сети становится всё более заметной, и расширение использования компьютеров заставляет пользователей позаботиться о проблемах безопасности компьютерных сетей, а также уделять больше внимания возможностям управления информационной безопасностью корпоративных сетей.

Очевидно, что ценность информации определяется в первую очередь приносимыми доходами. В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом «целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения» [1].

Основываясь на ключевых принципах шифрования данных, применяя знания криптографии, пользователи могут эффективнее решать вопросы информационной безопасности и безопасности операционной системы компьютера, предотвращая риски быстрого

Каримов Хасан Талхиевич
кандидат технических наук, старший преподаватель кафедры управления в органах внутренних дел, Уфимский юридический институт МВД России, город Уфа. Сфера научных интересов: информационные технологии, кибербезопасность, компьютерные науки и информатика. Автор более 80 опубликованных научных работ. SPIN-код: 1231-1706, AuthorID: 734720.
Электронный адрес: carimov.ces@mail.ru

Андрианов Владимир Александрович
преподаватель кафедры физической подготовки, Казанский юридический институт МВД России, город Казань. Сфера научных интересов: информационные технологии, кибербезопасность, компьютерные науки и информатика. Автор более 10 опубликованных научных работ. SPIN-код: 3399-3840, AuthorID: 588453.
Электронный адрес: wladimiraw@mail.ru

Пермяков Валерий Николаевич
кандидат технических наук, доцент кафедры прикладной механики и компьютерного инжиниринга. Башкирский государственный аграрный университет, город Уфа. Сфера научных интересов: информационные технологии, кибербезопасность, компьютерные науки и информатика. Автор более 100 опубликованных научных работ. SPIN-код: 2853-6350, AuthorID: 548037.
Электронный адрес: IR.PERM@yandex.ru

Тархова Ляйля Мукаддасовна
кандидат технических наук, доцент, доцент кафедры прикладной механики и компьютерного инжиниринга. Башкирский государственный аграрный университет, город Уфа. Сфера научных интересов: информационные технологии, кибербезопасность, компьютерные науки и информатика. Автор более 90 опубликованных научных работ. SPIN-код: 6387-9377, AuthorID: 448705.
Электронный адрес: tarkhova@ inbox.ru

Урманов Виль Губаевич
кандидат технических наук, доцент кафедры прикладной механики и компьютерного инжиниринга. Башкирский государственный аграрный университет, город Уфа. Сфера научных интересов: информационные технологии, кибербезопасность, компьютерные науки и информатика. Автор более 50 опубликованных научных работ. SPIN-код: 4735-0050, AuthorID: 574118.
Электронный адрес: uvg55@mail.ru

взлома и распознания конфиденциальной информации. Анализ текущей ситуации показывает важность информационной безопасности и необходимость усиления безопасности компьютерных сетей посредством шифрования данных.

Текущее состояние безопасности компьютерных сетей и необходимость ее усиления и совершенствования

В настоящее время уязвимость компьютерных сетей вызывает широкое беспокойство в обществе. В процессе использования объединенных в сеть компьютеров пользователи часто сталкиваются с риском кражи информации при обмене ключевыми данными, секретными материалами, конфиденциальной информацией. Компьютерная сетевая система уязвима для повреждения в общей среде, которая, несомненно, представляет большую

угрозу безопасности жизни и имуществу пользователей. При разработке компьютерных технологий решение вопроса сетевой уязвимости и безопасности стало предметом исследований. Безопасная передача, распределенная обработка, хранение, анализ данных и совместное использование ресурсов являются залогом эффективной работы компьютерной сети. Когда в этих функциях возникают уязвимости, работа компьютерной сети неизбежно столкнется с различными проблемами. Кроме того, важным компонентом компьютерной сети является различное программное и аппаратное обеспечение. Когда информация данных в этих аспектах подделывается или уничтожается, она также представляет угрозу безопасности компьютерной сети [2].

Активная атака и пассивная атака – два основных метода, используемых компьютерными хакерами для взлома компьютерных сетевых систем. Атака, влияющая на работу компьютерной системы или изменяющая системные ресурсы для достижения цели атаки, является активной. Пассивная атака – это взлом системы в целях завладеть какой-либо информацией без влияния на системные ресурсы. Кроме того, различные вирусы также представляют угрозу безопасности компьютерной сети. Компьютерные вирусы не только разнообразны, но и чрезвычайно сложны по структуре. Некоторые мутировавшие вирусы могут даже заражать основные файлы компьютера. Компьютерный вирус – это по своей сути вредоносный код, встроенный в компьютерные программы, который может повредить компьютерные данные. Безопасность компьютерной сети является предпосылкой для быстрого развития компьютерной техники. Защищенная компьютерная сеть может предоставить пользователям надежную информационную гарантию и автоматизировать рутинную работу, связанную с компьютерной сетевой системой, а также эффективно распределять роли в компьютерной сети, чтобы способствовать лучшему и быстрому развитию экономики и общества.

Анализ факторов, влияющих на безопасность компьютерных сетей

Для обеспечения безопасной работы компьютерной системы необходимо проанализировать факторы, которые влияют на безопасность компьютерной сети.

Сетевые вирусы. Сетевой вирус, затаившийся в компьютере пользователя, не только распространяется очень быстро, но также может нанести ущерб компьютеру. Сетевые вирусы созданы людьми, но они генерируются сами по себе, обладают сильной репликацией, силой восстановления и разрушительной силой, а также оказывают глубокое влияние на компьютеры пользователей. Распространенными сетевыми вирусами являются трояны и черви [3]. Эти два вируса имеют формы действия, отличные от других сетевых вирусов, и способы их атаки соответствуют изменениям для дифференцированных пользователей. Например, когда червь проникает в компьютер, он обычно удаляет исходные файлы в компьютерной системе, уничтожает компьютерные данные и делает компьютер полностью парализованным, вследствие чего последний не может продолжать нормально функционировать.

Запуск программы. Проблема с запущенной на компьютере программой связана с сетевой безопасностью – важным фактором, влияющим на операционную систему компьютера. Внимание и обеспечение безопасности работы компьютерной программы, регулярное техническое обслуживание и обновление программы не только улучшит работу компьютера, но и обеспечит основу безопасности компьютерной сети.

Взлом. Хакеры являются главными виновниками нарушения безопасности компьютерных сетей. При использовании компьютера и работы в сети хакеры пользуются уяз-

вимостями системы и недостатками, а также совершают решительные атаки и уничтожают данные. Для безопасного обслуживания компьютерной сети компьютерщики должны тратить много времени и сил, чтобы надолго предотвратить хакерские атаки. Обычно хакеры проникают в компьютер пользователя определенным способом атаки и получают ключи, данные информации системы посредством точного анализа и расчета. Затем, исходя из исследований и оценки результатов расчета, они выбирают определенные поведения атаки.

Технология шифрования для безопасности данных

С помощью алгоритма шифрования и секретного ключа открытый текст преобразуется в зашифрованный отправляющей стороной, а затем передается на принимающую сторону. Далее через алгоритм расшифровки и секретного ключа происходит восстановление зашифрованного текста до технологии открытого текста на принимающей стороне. При помощи различных технологий шифрования можно гарантировать защиту информации и безопасность современной компьютерной системы.

Шифрование и сокрытие – два основных средства технологии защиты данных. Полезная информация шифруется и передается в виде зашифрованного файла. Зашифрованная информация приходит к получателю в виде кода. Посредством использования электронного ключа пользователь расшифровывает полученную информацию и использует в своих целях. В случае перехвата информации злоумышленнику не удастся воспроизвести файл без специального электронного ключа. Тем не менее с помощью современных технологий и умений хакерам иногда удается завладеть данными. Во избежание возникновения такой ситуации вводятся новые средства защиты информации, например, появляющаяся в настоящее время технология шифрования и сокрытия будет передавать информацию без привлечения внимания злоумышленников, тем самым обеспечивая более высокую степень ее защиты во время коммуникационного процесса [4].

Классификация технологий шифрования данных

Как основная технология сетевой безопасности технология шифрования данных включает пять основных типов:

- шифрование узла;
- шифрование канала;
- сквозное шифрование;
- симметричное шифрование;
- асимметричное шифрование.

Технология шифрования узла. Этот вид технологии шифрования данных в основном опирается на канал связи для обеспечения безопасности данных информации. Технология шифрует все передаваемые данные, а прозрачное состояние пользователей в процессе шифрования дает промежуточным узлам сети возможность использовать разные ключи для шифрования информации, чтобы гарантировать, что передаваемая информация в узлах сети может быть представлена в форме зашифрованного текста. На основе расшифровки используются разные ключи для шифрования информации, что обусловливает существенную разницу между шифрованием узла и шифрованием канала.

Технология шифрования канала. Шифрование канала связи между двумя сетевыми узлами может эффективно защищать данные, передаваемые по сети. Благодаря применению технологии шифрования канала информация о данных должна передаваться через

несколько каналов связи, что, несомненно, значительно повышает безопасность процесса передачи информации.

Технология сквозного шифрования. Этот метод шифрования данных позволяет отображать данные полностью в зашифрованном виде во время передачи от отправителя к получателю. По сравнению с другими видами шифрования сквозное шифрование более простое в реализации, дизайне и поддержке. При применении технологии сквозного шифрования режим передачи сообщений, проходящих через сетевые узлы, должен определяться с помощью адреса назначения. По этой причине технология сквозного шифрования не может зашифровать адрес назначения информации, в связи с чем не может эффективно предотвратить ввод данных злоумышленниками в процессе передачи [5].

Технология симметричного шифрования. Техника шифрования и дешифрования данных с помощью того же ключа является симметричным шифрованием, также известным как ключевое шифрование. Алгоритм шифрования и ключ управления являются важными факторами, влияющими на безопасность симметричного шифрования. Так как данные шифрования и дешифрования должны использовать один и тот же ключ, это делает передачу ключа безопасности особенно критичным. Технология симметричного шифрования в основном включает в себя три общих алгоритма шифрования: AES-, IDEA- и DES-алгоритмы, среди которых наиболее используемый в повседневной работе алгоритм DES. Технология симметричного шифрования используется для шифрования двоичных данных, данных большого объема и в целом имеет широкий спектр применения, хороший прикладной эффект и значительное преимущество с точки зрения скорости шифрования [6].

Технология асимметричного шифрования. В отличие от симметричного шифрования асимметричное шифрование требует комбинации открытых и закрытых ключей для шифрования и расшифровки данных. Если данные зашифрованы с использованием открытого ключа, то расшифрованы они должны быть с использованием соответствующего закрытого ключа. Если данные зашифрованы с использованием закрытого ключа, то данные должны быть расшифрованы с использованием соответствующего открытого ключа. Асимметричное шифрование более безопасно, чем симметричное, поскольку используются два разных ключа, и менее вероятно, что информация о данных в процессе передачи будет взломана.

Ценность технологии шифрования данных

Непрерывные инновации в технологии шифрования данных играют всё бóльшую роль в эффективном повышении безопасности передачи данных по сети. В целом значение технологии шифрования данных отражается в следующих двух аспектах.

Во-первых, повышение уровня безопасности. Технология шифрования данных значительно повышает безопасность передачи данных, и, например, информация о движении денежных средств может быть защищена соответствующим уровнем безопасности компьютерной системы, что, в свою очередь, повысит доверие пользователей к безопасности компьютерной сети.

Во-вторых, можно оценить безопасность сети. Технология шифрования данных может показать уровень безопасности сетевых данных в процессе передачи информации и является важным показателем для оценки сетевой безопасности. Безопасность передачи данных – основа построения системы безопасности компьютерной сети. Чтобы обеспечить своевременную и точную передачу данных, агентства безопасности сети должны по-

стоянно обновлять технологии шифрования, повышать уровень безопасности и точности передачи данных.

Применение технологии шифрования данных в обеспечении безопасности компьютерных сетей

Улучшение шифрования данных. Преобразование данных информации открытого текста в зашифрованные данные осуществляется с помощью соответствующего криптографического алгоритма, что является фундаментальным моментом шифрования. Например, когда пользователи проводят транзакции в онлайн-банках и происходит утечка информации, система быстро примет соответствующие меры для обеспечения безопасной передачи данных по компьютерной сети.

Применение пакетного шифрования. Как наиболее распространенный метод шифрования данных пакетное шифрование со сжатием в основном включает ZIP и RAR. На основе установки пароля для расшифровки и использования зашифрованного пароля для точного получения соответствующей информации о компьютерных данных метод шифрования пакетов сжатия широко используется в сети почтовых перевозок. Применение компрессионного пакета шифрования может обеспечить эффективное сжатие почты и освобождение места на диске, улучшить общую эффективность работы компьютера.

Применение технологии шифрования узлов. Совершенствование и развитие компьютерной сети способствует эффективному применению технологии шифрования узла. Это основные предпосылки шифрования для обеспечения плавной синхронной или асинхронной линии для передачи данных между узлами. Кроме того, беспрепятственное выполнение работы по передаче информации также требует шифрования, чтобы промежуточные узлы сети имели соответствующие возможности обработки информационных данных. При этом узловое оборудование должно всегда поддерживать полностью синхронное состояние, и только таким образом можно предотвратить атаку хакеров, фальсификацию и кражу данных.

Применение технологии шифрования ссылок. С помощью технологии шифрования ссылок можно шифровать ссылки узлов компьютерной сети, обеспечивать безопасность и надежность передачи сетевой информации, шифровать данные, информацию перед передачей и выбирать различные типы ключей. Особенность технологии заключается в комплексе ссылок для шифрования и дешифрования, которые могут эффективно и всесторонне обеспечить безопасность передачи данных по сети.

Применение технологии сквозного шифрования. При применении технологии сквозного шифрования в процессе передачи зашифрованных данных от отправляющей стороны к принимающей нет необходимости проходить процедуры расшифровки каждой ссылки, поэтому сетевые данные могут быть хорошо защищены [7]. Применение технологии сквозного шифрования стало чрезвычайно популярным из-за таких ее преимуществ, как низкая стоимость, удобство в эксплуатации, постоянные инновации и оптимизация в процессе использования, а также возможность полного удовлетворения реальных потребностей пользователей.

Заключение

Способы обеспечения информационной безопасности могут быть подразделены на общие и частные, применение которых обусловливается масштабностью защитных действий. Разрушение важной информации, кража конфиденциальных данных, перерыв в ра-

боте вследствие отказа – всё это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей. Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются всё новые уязвимые места в программном обеспечении, приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных информационных систем; используются многочисленные внешние информационные сервисы; широкое распространение получило такое явление, как аутсорсинг, когда часть функций корпоративной информационной системы передается внешним организациям; развивается программирование с активными агентами.

Применение технологии шифрования для безопасности данных может обеспечить информационную безопасность компьютерной сети, способствует нормальной работе компьютерной системы, поэтому необходимо расширять исследования и разработки технологии шифрования данных, применять инновационные технологии шифрования данных и обеспечить научную теоретическую основу для поддержания безопасности компьютерных сетей.

Литература

1. Федеральный закон от 20.02.1995 N 24-ФЗ (ред. от 10.01.2003) «Об информации, информатизации и защите информации». Ст. 20. Цели защиты // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_5887/147785aa90796299e01fa06b3074fc435de917e6/?ysclid=lp8tnwjut4724656552 (дата обращения: 15.10.2022).

2. *Зенков А.В.* Информационная безопасность и защита информации : учебное пособие для вузов [Электронный ресурс]. М. : Юрайт, 2022. 104 с. (Высшее образование). URL: https://urait.ru/bcode/497002 (дата обращения: 15.10.2022).

3. *Чернова Е.В.* Информационная безопасность человека : учебное пособие для вузов [Электронный ресурс]. 2-е изд., испр. и доп. М. : Юрайт, 2022. 243 с. (Высшее образование). URL: https://urait.ru/bcode/495922 (дата обращения: 15.10.2022).

4. *Суворова Г.М.* Информационная безопасность : учебное пособие для вузов [Электронный ресурс]. М. : Юрайт, 2022. 253 с. (Высшее образование). URL: https://urait.ru/bcode/496741 (дата обращения: 15.10.2022).

5. *Казарин О.В., Шубинский И.Б.* Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования [Электронный ресурс]. М. : Юрайт, 2022. 342 с. (Профессиональное образование). URL: https://urait.ru/bcode/495524 (дата обращения: 15.10.2022).

6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов [Электронный ресурс] / Под ред. Т.А. Поляковой, А.А. Стрельцова. М. : Юрайт, 2022. 325 с. (Высшее образование). URL: https://urait.ru/bcode/498844 (дата обращения: 15.10.2022).

7. *Корабельников С.М.* Преступления в сфере информационной безопасности : учебное пособие для вузов [Электронный ресурс]. М. : Юрайт, 2022. 111 с. (Высшее образование). URL: https://urait.ru/bcode/496492 (дата обращения: 15.10.2022).

References

1. Federal Act of 20.02.1995 N 24-FZ (ed. of 10.01.2003) «On information, informatization and protection of information». Art. 20. Protection Objectives. *ConsultantPlus*. URL: https://www.consultant.ru/document/cons_doc_LAW_5887/147785aa90796299e01fa06b3074fc435de917e6/?ysclid=lp8tnwjut4724656552 (accessed 15.10.2022). (In Russian).
2. Zenkov A.V. (2022) *Informatsionnaya bezopasnost' i zashchita informatsii* [Information security and information protection]. Moscow : Yurait Publ. 104 p. URL: https://urait.ru/bcode/497002 (accessed 15.10.2022). (In Russian).
3. Chernova E.V. (2022) *Informatsionnaya bezopasnost' cheloveka* [Information security of man: Textbook for universities]. Moscow : Yurait Publ. 243 p. URL: https://urait.ru/bcode/495922 (accessed 15.10.2022) (In Russian).
4. Suvorova G.M. (2022) *Informatsionnaya bezopasnost'* [Information security]. Moscow : Yurait Publ. 253 p. URL: https://urait.ru/bcode/496741 (accessed 15.10.2022). (In Russian).
5. Kazarin O.V., Shubinsky I.B. (2022) *Osnovy informatsionnoi bezopasnosti: nadezhnost' i bezopasnost' programmnogo obespecheniya* [Fundamentals of information security: Reliability and security of software]. Moscow : Yurait Publ. 342 p. URL: https://urait.ru/bcode/495524 (accessed 15.10.2022). (In Russian).
6. Polyakova T.A., Streltsov A.A. (Eds.) (2022) *Organizatsionnoe i pravovoe obespechenie informatsionnoi bezopasnosti* [Organizational and legal support of information security]. Moscow : Yurait Publ. 325 p. URL: https://urait.ru/bcode/498844 (accessed 15.10.2022). (In Russian).
7. Korabelnikov S.M. (2022) *Prestupleniya v sfere informatsionnoi bezopasnosti* [Crimes in the field of information security]. Moscow : Moscow: Yurait Publ. 111 p. URL: https://urait.ru/bcode/496492 (accessed 15.10.2022). (In Russian).