УДК 004.89

Идрисова Ж.В.¹, Вагапова М.В.², Алихаджиев С.Х.³

СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

*¹кафедра «Программирование и инфокоммуникационные технологии»
факультета информационных технологий, ФГБОУ ВО «Чеченский
государственный университет» г. Грозный*

J120712@yandex.ru

*²студентка 2 курса факультета информационных технологий ФГБОУ ВО
«Чеченский государственный университет» г. Грозный*

maty.vgpn@mail.ru

*¹кандидат физико-математических наук кафедры «Программирование и
инфокоммуникационные технологии» факультета информационных
технологий, ФГБОУ ВО «Чеченский государственный университет»*

said366502@mail.ru

Аннотация. В данной статье раскрываются такие понятия, как информационная безопасность и сетевые информационные технологии. Здесь также говорится о наиболее популярных причинах утечки информации и решениях по их устранению. Рассмотрена DLP-система, как средство защиты информации и предотвращения утечек, в статье представлены основные компоненты и принцип работы системы DLP.

Ключевые слова: информационная безопасность, сетевые технологии, информационные сети, DLP-системы.

Idrisova J.V.¹, Vagapova M.V.² Alikhadzhiev S.Kh.³

NETWORK INFORMATION TECHNOLOGIES AND INFORMATION PROTECTION MEANS

*¹Department of Programming and Infocommunication Technologies, Faculty of
Information Technologies, Chechen State University, Grozny*

*²2nd year student of the Faculty of Information Technologies of the Chechen
State University of Grozny*

*³Candidate of Physical and Mathematical Sciences of the Department of
Programming and Information and Communication Technologies of the Faculty
of Information Technology, Chechen State University of Grozny*

Abstract. This article covers such concepts as information security and network information technology. It also discusses the most common causes of information leaks and solutions for eliminating them. DLP-system, as a means of

protecting information and preventing leaks, is considered, the article presents the main components and principle of operation of the DLP system.

Keywords: information security, network technologies, information networks, DLP systems.

Введение. На сегодняшний день, в результате информатизации и глобализации общества, информация стала одним из ценнейших ресурсов. Однако, желая приобрести ту или иную информацию, люди порой прибегают к незаконным способам, но и это не единственная угроза. Нередко также возникает утечка информации из системы, ввиду технических неполадок. Поэтому защита информации является одним из важнейших процессов в информационном обществе.

Целью данной статьи является знакомство с различными причинами утечки информации и способами их предотвращения.

Изложение основного материала. Информационная безопасность – это сохранность информации, а также защита прав человека и общества в информационном пространстве. Системы информационной безопасности должны содержать конфиденциальность, целостность и доступность информации. Угроза информации может быть случайной (сбой программы или сети, отключение энергии, неполадки в системе и т.п.) и преднамеренной (перехват информации, взлом системы и т.п.).

Наиболее удобный и быстрый способ передачи информации предоставили сетевые информационные технологии (которые впервые появились в 1960-е вместе с ЭВМ). Это такие технологии, которые объединяют в себе процессы сбора, обработки, передачи и хранения информации. Основу сетевых информационных технологий составляют информационные сети [4]. Информационные сети – это вид коммуникационной сети, которая выполняет все процессы, связанные с информацией, а также может проводить сетевые вычисления [4]. Не смотря на всю практичность сетевых технологий, именно она может стать причиной утечки информации вовне. Утечка информации – это утрата информации при электронном или физическом распространении [5].

Причинами утечки информации может быть перехват или сбой системы ввиду технической неполадки. Ко вторым можно отнести:
– человеческий фактор инсайдеров: незнание работниками правил пользования информацией и ее защиты, использование не аттестованных технических средств защиты информации, слабый контроль (или его отсутствие) за соблюдением правил информационной защиты и т.д.;

– непредвиденные факторы, независящие от организации: погодные условия, стихийные бедствия, катастрофы и неисправности или аварии технического оборудования.

Хоть это и сложно представить методы борьбы с последними факторами, но в связи с проблемой перехвата и неопытностью работников и получила распространение DLP-система в 2006 году.

DLP-системы (Data Leak Provention – одна из расшифровок, означающая «предотвращение утечек данных») – это программные устройства, предотвращающие утечку конфиденциальной информации за пределы организации или информационной структуры. DLP относится к программно-аппаратным средствам защиты информации [1]. Основными составляющими таких систем являются:

- модуль базы данных
- модуль анализа информации.

База данных необходима для хранения информации, начиная от ее контроля и подробной информации об инцидентах и заканчивая документами, попавшими в поле зрения системы. Модули анализа отвечают за анализ всей информации, извлеченной из разных источников. Существуют и специальные агенты, которые следят за действиями инсайдеров конкретной системы, оставаясь пассивным при их работе и активно препятствуя их несанкционированным действиям. Модуль, производящий мониторинг функционирования и администрирования DLP-системы называется модуль управления.

На сегодняшний день продукты данной системы защищают не только от утечки информации, но и от внешних и внутренних угроз, а также обеспечивают контроль над всеми действиями на рабочих станциях, включая даже удаленную работу.

DLP-системы можно разделить в соответствии со способами обнаружения утечки данных:

Data-in-Use – при использовании на рабочем месте пользователя;

Data-in-Motion – при передаче в сети компании;

Data-at-Rest – при хранении на серверах и рабочих станциях компании [2, 3].

Выводы. Несмотря на то, что DLP-системы претерпели достаточно много улучшений для качественной защиты от утечки информации, даже при их контроле данные могут потеряться. Но с каждым разом, наряду с другими способами защиты информации, эта система развивается и совершенствуется. Однако даже с уже существующими возможностями предотвращения угроз, я считаю, что проблема защиты информации будет

актуальной до тех пор, пока существует информационное общество. Вероятность сбоя системы присутствует всегда, а кроме этого, как сказал Натан Майер Ротшильд «Кто владеет информацией, тот владеет миром», а проблема желания получить большее заложена глубоко в человеческом сознании.

Литература

1. Обзор DLP-систем 08.02.2016 // СёрчИнформ Обеспечение информационной безопасности // URL: <https://searchinform.ru/blog/2016/02/08/obzor-dlp-sistem/>
2. Шихов Е. Обзор DLP-систем на мировом и российском рынке // Профессиональная конференция по управлению ИБ – август 2014 // URL: https://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014
3. Система информационной безопасности // Твой Бизнес – онлайн журнал 2015 // URL: <https://tvoi.biz/biznes/informatsionnaya-bezopasnost/sistema-informatsionnoj-bezopasnosti.html>
4. Информационные технологии в обучении студентов, Ж.В. Идрисова, Известие Чеченского государственного университета №3(7), 2017 г. https://elibrary.ru/download/elibrary_32278179_77436501.pdf
5. Сетевые информационные технологии // StudFiles 03.2015 // URL: <https://studfiles.net/preview/2687586/page:67/>
6. Ерыгин А.В. Анализ эффективности систем предотвращения утечек конфиденциальной информации из локальных сетей // КиберЛенинка – научная электронная библиотека // URL: <https://cyberleninka.ru/article/n/analiz-effektivnosti-sistem-predotvrascheniya-utechek-konfidentsialnoy-informatsii-iz-lokalnyh-setey>