АНАЛИЗ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ

Табилова А.З.[1], Коннов А.Л.[2] Email: Tabilova671@scientifictext.ru

[1]Табилова Альфия Загитовна – магистр,
направление: управление и информационные технологии в технических системах;
[2]Коннов Андрей Леонидович - кандидат технических наук, доцент,
кафедра управления и информатики в технических системах,
Оренбургский государственный университет
г. Оренбург

Аннотация: *в статье рассмотрена актуальность проблемы информационной безопасности в корпоративных сетях. Далее будут проанализированы проблемы защиты конфиденциальной информации и способы их решения в рамках организации корпоративных сетей. Раскрыты причины нарушения безопасности в корпоративной среде и актуальные способы их устранения и усложнения получения доступа к конфиденциальной информации организации, такие как: институциональные методы, антивирусное программное обеспечение (ПО), межсетевые экраны, системы обнаружения атак и VPN. Определены важнейшие вирусные нападения, имеющие большое влияние на производительность корпоративных сетей, которые влекут за собой потенциальную угрозу утери или дублирования закрытых корпоративных данных, воздействие вредоносного ПО на потенциальный ресурс предприятия. Также была предложена к рассмотрению альтернативная методика борьбы с угрозами.*

Ключевые слова: *программное обеспечение, корпоративные сети.*

ANALYSIS OF INFORMATION SECURITY PROBLEMS IN CORPORATE NETWORKS

Tabilova A.Z.[1], Konnov A.L.[2]

[1]Tabilova Alfiya Zagitovna– Masters,
DIRECTION: MANAGEMENT AND INFORMATION TECHNOLOGY IN TECHNICAL SYSTEMS;
[2]Konnov Andrey Leonidovich - Candidate of technical sciences, Associate Professor,
DEPARTMENT OF MANAGEMENT AND INFORMATICS IN TECHNICAL SYSTEMS,
ORENBURG STATE UNIVERSITY,
ORENBURG

Abstract: *the article addresses security issues. Next, we will analyze the problems of protecting confidential information and how to solve them within the organization of corporate networks. Disclosing the causes of security breaches in the corporate environment and providing access to confidential information of organizations, such as: institutional methods, antivirus software (software), firewalls, attack detection systems and VPNs. The most important virus attacks have been identified that have a large impact on the performance of corporate networks, which entail a potential threat of loss or duplication of closed corporate data, the impact of malware on a potential resource of the enterprise. An alternative methodology for combating threats was also proposed for consideration.*

Keywords: *software, corporate networks.*

УДК 004.5

Цель работы — анализ эффективных методов обеспечения защиты корпоративных информационных сетей.

Научно-технологический прогресс стремительно набирает обороты, создавая новые решения и сталкивая нас с новыми проблемами. Оптимизация информационных технологий влияет на производительность работы за счет цифровых копий данных. Они лидируют по ряду преимуществ перед физическим носителем. Например, копии имеют долгосрочное хранение без износа конечного информационного источника, сохранение физического пространства и т.д.

Для осуществления управления в современных реалиях защита информации является одном из важнейших аспектов. Этот факт нужно учитывать на всех этапах функционирования корпоративных сетей. Перед нами стоит задача, усовершенствования корпоративной сети передачи данных машиностроительного завода. Именно она больше всего подвергается угрозам, так как через неё идет поток информации, необходимый для деятельности предприятия. Если представить, что работа сети будет приостановлена, то из этого будет следовать, что вся бухгалтерская, производственная деятельность будет парализована, что для предприятия может повлечь за собой большие убытки.

Информационная безопасность должная основываться на защите информации, которая имеет возможность параллельной работы нескольких программно-аппаратных решений, которые поддерживают и дополняют друг друга. Таким образом, специалисты должны понимать, что правильное применение современных технологий защиты корпоративной информации - это залог успешной работы предприятия, и пренебрежение им ведет к негативным финансовым и имиджевым последствиям.

Давно уже стало известным фактом то, что главной угрозой для информационных систем - является вирус (троянское ПО, черви), так же значительный вред приносит и шпионское ПО, спам. Приведем пример фишинг-атаки (Рис. 1) (вид интернет мошенничества, целью которого является получение доступа к конфиденциальной информации), социальный инжиниринг [1].

Общая схема фишинговой атаки

Рис. 1. Общая схема фишинговой атаки

Так же немаловажный фактор в обеспечении безопасности системы составляют сотрудники организации. Неграмотно использование, например, почтовых сервисов может привести к проникновению вируса во всю систему, так как рассылка вредоносных программ через e-mail сообщения - одно из распространенных видов атаки. Вредоносные алгоритмы влекут за собой полную остановку системы, утрачивание и утечку данных, сбой.

Для обеспечения безопасности данных существуют методы защиты информации как: создание межсетевых экранов, криптография, аутентификация, регистрация, протоколирование и управление доступом.

Стоит отметить, что информационная безопасность также обеспечивается и государством, что отражается в требованиях нормативно-правовых актов, таких как:

1. Гражданский кодекс РФ.
2. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписке».
3. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 29.06.2004 г. № 98-ФЗ «О коммерческой тайне».

Контролирующими органами информационной безопасности в Российской Федерации являются: Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности, Федеральная служба охраны, Министерство обороны РФ, Министерство связи и массовых коммуникаций РФ, Служба внешней разведки РФ и Банк России. Конечно, государство не способно предоставить полную защиту информации для организации, поэтому, каждой организации следует самой заботится о безопасности информации [2].

Меры, способствующие защите данных:

– создать политику безопасности и составить соответствующую документацию;

– внедрить технические средства защиты информации [3].

Для создания защиты системы на предприятии применяются технологии антивирусной защиты. Модуль межсетевого экранирования и криптографической защиты трафика при его передаче на сетевом уровне обеспечивает защиту рабочих станций, кодирует почтовые шлюзы, прокси-серверы и иные вариации проникновения вирусов. В отличие от частного использования, в корпоративных сетях результативным решением является применение, например, двух или более антивирусных программ, что сократит диапазон возможных угроз [4].

Повышению безопасности информации также способствует контроль доступа и средств защиты информации внутри сети. На предприятиях для повышения безопасности создается автоматизированная система управления информационной безопасностью. Вход в сеть определяется согласно должностным инструкциям и области работы. Для решения данного вопроса применяется виртуальная частная сеть VPN, которая кодирует трафик внутри организации [5].

Так же есть выбор из уже существующих систем обеспечения безопасности информации. Например, рассмотрим «DENUVO» - это технология защиты от несанкционированного взлома, разработанная австрийской компанией «Denuvo Software Solutions GmbH». «DENUVO» шифрует и расшифровывает с хаотичной периодичностью, что способствует уменьшению риска взлома. Данная система была взломана лишь один раз. «DENUVO» занимает лидирующие позиции на рынке услуг по защите [6].

В данной статье были описаны основные проблемы информационной безопасности в корпоративных сетях. Вследствие чего сети подвергаются большому количеству угроз - вирусных атак и угроз на основе человеческого фактора.

Цель статьи была раскрыта и проанализированы методы, такие как: антивирусное ПО, системы обнаружения атак и т.д. Данный комплекс способствует снижению риска несанкционированного доступа к рабочей информации и оптимизации общего рабочего процесса. Была предложена система «DENUVO», которая способна увеличить эффективность комплекса защиты.

Список литературы / References

1. АО «Лаборатория Касперского»: официальный сайт. [Электронный ресурс]. Режим доступа: https://securelist.ru/statistics/ (дата обращения: 30.08.2019).
2. Гражданский кодекс Российской Федерации: Часть первая – четвертая: [Принят Гос. Думой 23 апреля 1994 года, с изменениями и дополнениями по состоянию на 10 апреля 2009 г.] // Собрание законодательства РФ, 1994. № 22. Ст. 2457.
3. *Кубаренко А.С.* Модернизация корпоративной компьютерной сети предприятия // Научно-методический электронный журнал «Концепт», 2016. Т. 11. С. 3131–3135. [Электронный ресурс]. Режим доступа: http://e-koncept.ru/2016/86662.htm/ (дата обращения: 30.08.2019).
4. *Олифер В., Олифер Н.*. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2013. 944 с.
5. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. М.: ДМК Пресс, 2008. 544 с.
6. Denuvo. [Электронный ресурс]. Режим доступа: https://irdeto.com/video-entertainment/piracy-control/ (дата обращения: 30.08.2019).