УДК 005.7:004.056+338.2-049.5

ПРОВЕДЕНИЕ ПРОВЕРКИ УЯЗВИМОСТЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ КОМПАНИИ КАК СПОСОБ ПОВЫШЕНИЯ ЕЁ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Мэн Цзыминь

магистрант Белорусского государственного университета, г. Минск, Республика Беларусь, e-mail: mengzimin1201@gmail.com

Научный руководитель: **А. А. Быков**

доктор экономических наук, профессор, Белорусский государственный экономический университет, экономический факультет, г. Минск, Республика Беларусь, e-mail: aliaksei.bykau@yandex.ru

В данной статье исследуются проблемы обеспечения экономической безопасности компаний в условиях поступательного развития цифровой экономики, которые приобретают для них особую значимость. Создание и обеспечение непрерывного функционирования систем защиты информации в целях выполнения правил экономической безопасности требует всё больших расходов компаний. Особенно явно рассматриваемая проблема присутствует в отношении небольших и средних компаний. Предлагается привлечение к проверке уязвимостей компьютерных сетей компании «этичных хакеров», – специалистов по тестированию безопасности компьютерных систем путем попытки их взлома. Проведение проверок уязвимостей корпоративных компьютерных сетей, особенно для малых и средних компаний, путем попытки их взлома «этичными хакерами» является эффективным способом повышения экономической безопасности компаний.

Ключевые слова: информационная безопасность; уязвимости компьютерных систем; инструменты повышения безопасности; несанкционированный доступ; экономическая безопасность.

CHECKING THE VULNERABILITIES OF A COMPANY'S COMPUTER SYSTEMS AS A WAY TO INCREASE ITS ECONOMIC SECURITY

Meng Zimin

master student of the Belarusian State University, Minsk, Republic of Belarus, e-mail: mengzimin1201@gmail.com

Supervisor: **A. A. Bykov**

doctor of economics, professor, Belarus State Economic University, Minsk, Republic of Belarus, e-mail: aliaksei.bykau@yandex.ru

This article examines the problems of ensuring the economic security of companies in the context of the progressive development of the digital economy, which are of particular

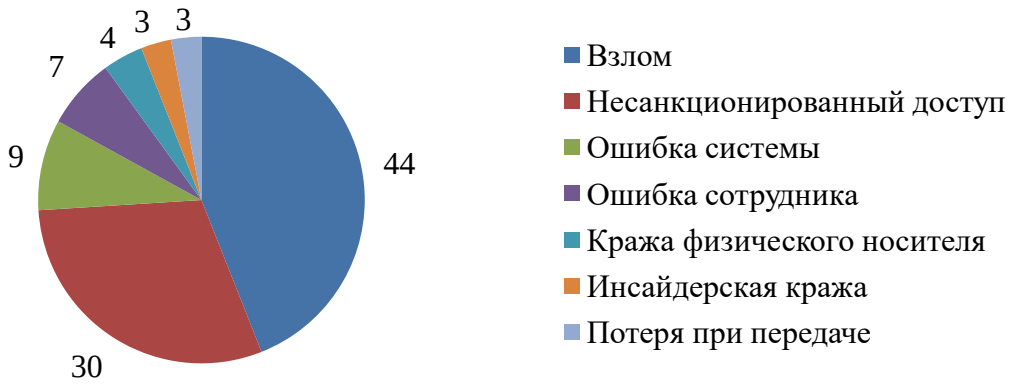
importance for them. The creation and maintenance of continuous operation of information security systems in order to comply with the rules of economic security requires more and more expenses for companies. This problem is especially evident in relation to small and medium-sized companies. It is proposed to involve «ethical hackers» in checking the vulnerabilities of the company's computer networks – specialists in testing the security of computer systems by attempting to hack them. Conducting vulnerability checks of corporate computer networks, especially for small and medium-sized companies, by attempting to break them by «ethical hackers» is an effective way to increase the economic security of companies.

Keywords: information security; computer system vulnerabilities; security enhancement tools; unauthorized access; economic security.

Обеспечение экономической безопасности компаний в условиях поступательного развития цифровой экономики приобретает для них особую значимость. Именно информационная безопасность становится в современных условиях первостепенным стабилизирующим фактором при формировании комплексной системы экономической безопасности компании.

В условиях всё большего развития цифровой экономики в деятельности компаний происходит объективный рост использования информации, компьютерных средств и компьютерных сетей и т. д. При этом прогрессирует легкость доступа к конфиденциальной бизнес-информации не только персонала конкретной компании, но и её конкурентов и других нежелательных лиц.

В соответствии с данными, полученными в ходе исследования Identity Theft Resource Center (ITRC) нежелательные причины утечки корпоративной конфиденциальной бизнес-информации распределяются следующим образом (рисунок).



Распределение причин утечки корпоративной конфиденциальной бизнес-информации

Источник [1].

На 1-м месте причин является взлом компьютерных сетей (44 %), на 2-м – несанкционированный доступ к корпоративной компьютерной системе (30 %) и только далее следуют непреднамеренные действия: ошибки системы (9 %), ошибки сотрудников компании (7 %). В целом, по данным ITRC в связи с преднамеренными и незаконными действиями злоумышленников по причине взломов и краж происходит свыше 80 % случаев утечки конфиденциальной бизнес-информации [1].

Кроме того, преднамеренные действия по созданию угроз утечки информации увеличиваются не только количественно, но и качественно, что связано с опережающим развитием IT-технологий в мире.

Компании в целях минимизации ущерба вынуждены постоянно совершенствовать защиту конфиденциальной информации путем её шифрования, использования многофакторной идентификации, обучения персонала действиям в условиях информационной безопасности и т. д. [2].

Создание и обеспечение непрерывного функционирования комплексных систем защиты информации в целях выполнения правил экономической безопасности требует всё больших расходов компаний. Особенно явно рассматриваемая проблема присутствует в отношении небольших и средних компаний, которые не могут позволить себе создание и обеспечение деятельности собственных служб информационной безопасности. Компании в своем большинстве всё равно остаются уязвимыми перед угрозами утечки конфиденциальной информации.

В то же время заслуживает внимание метод привлечения к проверке уязвимостей компьютерных сетей компании так называемых «этичных хакеров», – специалистов по тестированию безопасности компьютерных систем путем попытки их взлома. Цель попытки взлома – последующая помощь в разработке более надежной защиты конфиденциальной информации.

Идея использования «этического взлома» как инструмента повышения безопасности компьютерных сетей компаний была предложена «этичными хакерами» Дэном Фармером и Виетсом Венема, которые разработали первую в данной сфере программу «Инструмент администратора безопасности для анализа сетей» SATAN.

Одна из самых известных и популярных платформ «этичных хакеров» HackerOne за 10 лет своего существования помогла найти в корпоративных сетях и устранить более 230 тыс. уязвимостей, а общая сумма выплат пентестерам (специалистам, которые находят уязвимости) превысила 200 млн долл. США [3]. Число компаний, желающих находить уязвимости в корпоративных системах безопасности увеличивается: за 2022 г. их стало почти на 20 % больше. В ежегодном отчете сервиса HackerOne за 2021 г. отмечается, что специалисты получили выплаты на сумму около 40 млн долл. США [3].

В настоящее время на рынке присутствуют предложения по проверке уязвимостей компьютерных систем компаний путем попытки их взлома как от отдельных специалистов в данной сфере («белых хакеров»), так и от специализированных фирм. Условия их работы максимально прозрачны.

Проведение проверок уязвимостей корпоративных компьютерных сетей, особенно для малых и средних компаний, путем попытки их взлома «этичными хакерами» является эффективным способом повышения экономической безопасности компаний.

Библиографические ссылки

5. ITRC End-of-Year Data Breach Report // Identity Theft Resource Center [Электронный ресурс]. URL: https://www.idtheftcenter.org/wpcontent/uploads/ITRC (дата доступа: 10.02.2023).

6. *Русакович И. С., Бокунович Т. А.* Информационная безопасность как элемент экономической безопасности предприятия [Электронный ресурс] / Электронная библиотека БГУ. URL: https://elib.bsu.by/handle/123456789/260073 (дата доступа: 01.02.2023).

7. Сайт Myfin.by[Электронный ресурс]. URL: https://myfin.by/stati/view/stat-millionerom-za-god-kto-takie-belye-hakery-i-skolko-oni-zarabatyvaut (дата доступа: 13.02.2023).