ЭКОНОМИКА
ECONOMICS

DOI: 10.18287/2542-0461-2023-14-2-7-16

НАУЧНАЯ СТАТЬЯ

УДК 338.2

Дата поступления: 16.02.2023
рецензирования: 24.03.2023
принятия: 30.05.2023

Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации

С.В. Афанасьева
Санкт-Петербургский государственный экономический университет,
г. Санкт-Петербург, Российская Федерация
E-mail: afanasyeva_svtln@mail.ru. ORCID: https://orcid.org/0009-0003-0821-2876
Е.С. Черепанова
Санкт-Петербургский государственный экономический университет,
г. Санкт-Петербург, Российская Федерация
E-mail: ms.Katusha01.06@mail.ru. ORCID: https://orcid.org/0009-0000-2480-1513
Н.В. Шехова
Балтийский государственный технический университет «Военмех» имени Д.Ф.Устинова,
г. Санкт-Петербург, Российская Федерация
E-mail: nataly65vf@gmail.com. ORCID: https://orcid.org/0000-0002-4904-7120

Аннотация: В статье представлены результаты исследования теоретических, методологических, институциональных, технических и правовых аспектов проблемы предотвращения угроз кибербезопасности в организации, занимающих важнейшее место в системе обеспечения экономической безопасности. Авторы выявили и описали основные киберугрозы в компании. К ним можно отнести: распространение компьютерных вирусов, рассекречивание информации, являющейся важной для организации, кража данных с помощью методов конкурентной разведки, непредумышленные ошибки работников, которые в дальнейшем привели к техническим сбоям в работе программного обеспечения. Также были выявлены возможные негативные последствия: уменьшение доходов организации от потери прибыли, распространение конфиденциальной информации и коммерческой тайны, подрыв общественного мнения и снижение авторитета компании, потеря клиентов. Были рассмотрены наиболее распространенные виды кибератак, к числу которых относятся DDoS-атака, фишинг, вредоносное программное обеспечение, социальная инженерия, смишинг, утечка данных, Brute-force. Авторами представлены результаты анализа статистических данных за 2021 и 2022 гг. по числу утечек, распределению их по виновникам, по категориям жертв среди организаций. На основе разработанной авторами анкеты был проведен опрос, который позволил выявить основные угрозы кибербезопасности в организации. Разработан и предложен перечень мероприятий по нейтрализации и минимизации киберугроз в компании, которые вполне правомерно рассматривать в качестве инновационных методов их предотвращения для обеспечения экономической безопасности. В основу мероприятий по предотвращению киберугроз вошли следующие: постоянная оценка возможных рисков и своевременное обновление информационных баз и систем, внедрение активной программы обучения для сотрудников организации, создание плана по реагированию на кибератаки. В качестве информационной базы для написания данной статьи выступили научные работы отечественных и зарубежных ученых. Кроме того, авторы ссылались на данные экспертно-аналитического центра InfoWatch, FBK CyberSecurity и Positive Technologies.

Ключевые слова: экономическая безопасность; информационная безопасность; киберугрозы; кибербезопасность; утечка данных; вирусы; вредоносное ПО; хакеры; киберриски; DDoS-атака.
Цитирование. Афанасьева С.В., Черепанова Е.С., Шехова Н.В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации // Вестник Самарского университета. Экономика и управление. 2023. Т. 14, № 2. С. 7–16. DOI: http://doi.org/10.18287/2542-0461-2023-14-2-7-16.
Информация о конфликте интересов: авторы заявляют об отсутствии конфликта интересов.

Светлана Валерьевна Афанасьева – студентка факультета бизнеса, таможенного дела и экономической безопасности, Санкт-Петербургский государственный экономический университет, 191023, Российская Федерация, г. Санкт-Петербург, ул. Садовая, 21.

Екатерина Сергеевна Черепанова – студентка факультета бизнеса, таможенного дела и экономической безопасности, Санкт-Петербургский государственный экономический университет, 191023, Российская Федерация, г. Санкт-Петербург, ул. Садовая, 21.

Наталия Владимировна Шехова – доктор экономических наук, профессор кафедры Р 1 «Менеджмент организации», профессор, Балтийский государственный технический университет «Военмех» имени Д.Ф. Устинова, 190005, Российская Федерация, г. Санкт-Петербург, ул. 1-я Красноармейская, 1.

SCIENTIFIC ARTICLE

Submitted: 16.03.2023
Revised: 24.03.2023
Accepted: 30.05.2023

Innovative methods for cyber threats prevention to ensure the economic security of organizations

S.V. Afanasyeva
Saint-Petersburg State University of Economics, Saint Petersburg, Russian Federation
E-mail: afanasyeva_svtln@mail.ru. ORCID: https://orcid.org/0009-0003-0821-2876
E.S. Cherepanova
Saint-Petersburg State University of Economics, Saint Petersburg, Russian Federation
E-mail: ms.Katusha01.06@mail.ru. ORCID: https://orcid.org/0009-0000-2480-1513
N.V. Shekhova
Baltic State Technical University «Voenmeh» named after D.F. Ustinov,
Saint Petersburg, Russian Federation
E-mail: nataly65vf@gmail.com. ORCID: https://orcid.org/0000-0002-4904-7120

Abstract: The article presents the results of a study of theoretical, methodological, institutional, technical and legal aspects of the problem of preventing cybersecurity threats in the organization, which occupy a crucial place in the system of economic security. The authors identified and described the main cyber threats in the company. These could include: the spread of computer viruses, the declassification of information that is important to the organization, data theft through competitive intelligence methods, unintentional mistakes of employees, which subsequently led to technical failures in the software. Possible negative consequences were also identified. As they were presented as the following: reduction of the organization's income from loss of profit, dissemination of confidential information and trade secrets, undermining of public opinion and reduction of the company's credibility, loss of customers. The paper considered the most common types of cyberattacks, which include DDoS-attack, phishing, malware, social engineering, smishing, data leakage, Brute-force. The authors present the results of an analysis of statistical data for 2021 and 2022 on the number of leaks, their distribution by perpetrator, by victim category among organizations. Based on the questionnaire developed by the authors, a survey was conducted to identify the main threats to cybersecurity in the organization. The article developed and proposed a list of measures to neutralize and minimize cyber threats in the company, which is legitimate to consider as innovative methods of their prevention to ensure economic security. The basis of measures to prevent cyber threats included the following: constant assessment of possible risks and timely updating of information bases and systems, the introduction of an active training program for employees of the organization, the creation of a plan to respond to cyber-attacks. Scientific works of domestic and foreign scientists were used as an information base for

writing this article. In addition, the authors referred to data from the InfoWatch Center for Expert Analysis, FBK CyberSecurity and Positive Technologies.
Key words: economic security; information security; cyber threats; cyber security; data leakage; viruses; malware; hackers; cyber risks; DDoS attack.
Citation. Afanasyeva S.V, Cherepanova E.S., Shekhova N.V. Innovative methods for cyber threats prevention to ensure the economic security of organizations. *Vestnik Samarskogo universiteta. Ekonomika i upravlenie = Vestnik of Samara University. Economics and Management*, 2023, vol. 14, no. 2. pp. 7–16. DOI: http://doi.org/10.18287/2542-0461-2023-14-2-7-16. (In Russ.)
Information on the conflict of interest: authors declare no conflict of interest.

Svetlana V. Afanasyeva – student of the Faculty of Business, Customs and Economic Security, Saint Petersburg State University of Economics, 21, Sadovaya Street, Saint Petersburg, 191023, Russian Federation.
Ekaterina S. Cherepanova – student of the Faculty of Business, Customs and Economic Security, Saint Petersburg State University of Economics, 21, Sadovaya Street, Saint Petersburg, 191023, Russian Federation
Nataliya V. Shekhova – Doctor of Economics, professor of the Department of Organisation Management, professor, Baltic State Technical University «Voenmeh» named after D.F. Ustinov, 1, Pervaya Krasnoarmeyskaya Street, Saint Petersburg, 190005, Russian Federation.

Введение

Современные угрозы кибербезопасности, будучи непосредственно связанными с информационными рисками, занимают важнейшее место при решении вопросов обеспечения национальной безопасности вообще и экономической безопасности в частности. Вызовы, опасности, угрозы и риски, возникающие в настоящее время в информационной сфере, заставляют искать все новые взаимосвязи между названными категориями и разрабатывать инновационные методы предотвращения и реагирования. Сегодня роль и место информационной безопасности в системе национальной безопасности страны крайне велики. В современной научной повестке находится самый разнообразный спектр вопросов информационной безопасности и киберугроз: финансовые [1], правовые [2; 3], институциональные [4], технические [5] и др.

В современной научной литературе также публикуются работы, посвященные оценке эффективности государственного программно-целевого планирования в области информационной безопасности, выявление проблемных зон в этой сфере [6].

С каждым годом организации становятся все более уязвимыми к киберугрозам в связи с растущей зависимостью от компьютеров, профессиональных сетей, программ, социальных сетей и данных во всем мире. Изменение, уничтожение и распространение персональной информации – одна из самых популярных кибератак, которая имеет масштабные негативные последствия для бизнеса и часто возникает из-за недостаточно защищенных данных.

Сегодня можно говорить о постоянно возрастающем риске кибератак для организации, обусловленном с развитием глобальной связи и все увеличивающимися масштабами использования облачных сервисов, характеризующихся сравнительно низкими стандартными параметрами безопасности. Если раньше многие проблемы традиционно можно было решить посредством управления IT-рисками и контроля доступа, то теперь необходимо также нанимать новых специалистов по кибербезопасности, разрабатывать и устанавливать инновационное программное обеспечение и создавать систему управления рисками кибербезопасности. Каждая организация должна иметь стратегию снижения рисков и план реагирования на киберинциденты на случай взлома.

Сильная стратегия кибербезопасности может обеспечить хорошую защиту от вредоносных атак, направленных на доступ, изменение, удаление, уничтожение или вымогательство систем и конфиденциальных данных организации или пользователя. Кибербезопасность также играет важную роль в предотвращении атак, направленных на отключение или нарушение работы системы или устройства.

Кибербезопасность является в современных условиях одним из важнейших направлений информационной безопасности. Она подразумевает защищенность таких подключенных к Интернету систем, как оборудование, программное обеспечение, данные от киберугроз. Низкий уровень кибербезопасности может привести к проблемам с технической инфраструктурой, использованием технологий или репутацией организации, что является рисками кибербезопасности [1; 7].

Риск кибербезопасности – это возможные убытки в результате кибератаки или утечки данных в компании [8].

Кибербезопасность, по сути дела, представляет собой одну из технологий, лежащих в сфере практик и процессов, предназначенных для защиты интеллектуальной собственности организации, персональных и иных данных о клиентской базе, а также другой конфиденциальной информации от несанкционированного доступа киберпреступников. Поскольку частота и серьезность киберпреступлений неуклонно растут, значительно увеличивается потребность в улучшенном управлении рисками кибербезопасности как части профиля корпоративных рисков каждой организации. Независимо от склонности компании к риску планирование кибербезопасности необходимо включать как в процесс управления рисками предприятия, так и в обычные бизнес-операции.

Ход исследования

На основе анализа информации, представленной в отчете экспертно-аналитического центра InfoWatch об утечке данных за 1-е полугодие 2022 года, можно сказать, что по сравнению с 2021 годом количество утечек данных выросло примерно в 2 раза в мире и в 1,5 раза в России. В первом полугодии 2022 года число утечек в России составило 305 (см. рисунок 1). При этом более 80 % утечек информации были совершены с помощью хакерских атак. Не обошли стороной и кражи персональных данных из организаций, их число составило 186,7 млн записей по всей России. В число крупных организаций, которые претерпели утечки данных, вошли авиакомпания «Победа», сервисы курьерской службы «Яндекс Еда», Delivery Club, Почта России, СДЭК и другие [9; 10].

Рисунок 1 – Число утечек в 2021 и в 2022 гг.
Figure 1 – The number of leaks in 2021 and in 2022.

Проанализировав статистику лиц, причастных к утечке информации (см. рисунки 2, 3), можно сказать, что в 2021 году основными виновными были непривилегированные сотрудники, а также хакеры и другие неизвестные лица. Что касается 2022 года, то здесь возросла роль хакеров, которые были причастны к краже и утечке данных. Объяснением этому служит появление новых инструментов и способов для совершения вредоносных действий [9; 10].

Согласно данным статистики сайта Positive Technologies, в 2022 году основными категориями «жертв» утечек данных среди организаций являются государственные учреждения и предприятия сферы промышленности (значения показателя составили 18 и 13 % соответственно). Наименьшему количеству атак подверглись IT-компании и предприятия сферы услуг (5 и 4 % соответственно) (см. рисунок 4) [11]. Это можно объяснить тем, что госучреждения и сфера промышленности имеют большое количество уязвимостей в системах, которым не уделяется должного внимания. Что касается сферы услуг, то она является непривлекательной отраслью для хакеров, тогда как IT-компании имеют более надежную защиту своих систем.

Для того чтобы наглядно показать, как часто компании сталкиваются с кибератаками, авторами был проведен опрос. В качестве опрошенных выступили работники таких организаций, как АО «ЗАСЛОН», ООО «НПФ «Хеликс» и ООО «Газинформсервис». Для проведения опроса была сформирована следующая анкета (см. таблицу 1).

Рисунок 2 – Распределение утечек по виновным в 2021 г.
Figure 2 – Distribution of leaks by culprits in 2021

Рисунок 3 – Распределение утечек по виновным в 2022 г.
Figure 3 – Distribution of leaks by culprits in 2022

Рисунок 4 – Распределение утечек по отраслям в 2022 г.
Figure 4 – Distribution of leaks by industry in 2022

Таблица 1 – Анкета
Table 1 – Questionnaire

Вопрос	Варианты ответа
1) Были ли обнаружены Вами вирусы на рабочем персональном компьютере (ПК)?	А) Да Б) Нет
2) Позволяет ли система безопасности Вашего ПК скачать различные файлы на рабочий стол компьютера?	А) Да, можно скачать абсолютно все Б) Нет, нельзя
3) Каковы Ваши действия по окончании лицензии антивирусных программ?	А) Нажимаю на крестик, чтобы напоминание не отвлекало Б) Пытаюсь самостоятельно обновить лицензию В) Приглашаю специалистов из технического отдела
4) Как часто специалисты из технического отдела проводят диагностику Вашего рабочего ПК?	А) 1 раз в 3 месяца Б) 2 раза в 1 месяц В) Другое* *Если другое, то как часто? Ответ: _____
5) Пытались ли Вас когда-нибудь «взломать» на рабочем ПК?	А) Да Б) Нет
6) По Вашему мнению, как бы Вы оценили по 5-балльной шкале защиту данных в Вашей компании?	0 – нет никакой защиты данных на рабочем компьютере ... 5 – крайне высокая защита данных Ответ: _____ Обоснуйте свой ответ.

Источник: составлено авторами.

Результаты опроса, проведенного авторами статьи, представлены в таблице 2.

Таблица 2 – Результаты анкетирования
Table 2 – Survey results

Опрошенные	Обнаружение вирусов на рабочем ПК	Доступ к скачиванию на рабочем ПК	Действия по окончании лицензии на рабочем ПК	Частота диагностики рабочего ПК	Попытка взлома рабочего ПК	Оценка защиты данных на рабочем ПК
АО «ЗАСЛОН»	Да – 25 % Нет – 75 %	Да – 0 % Нет – 100 %	А – 25 % Б – 50 % В – 25 %	А – 0 % Б – 0 % В – 100 %	Да – 50 % Нет – 50 %	1 – 0 % 2 – 0 % 3 – 25 % 4 – 25 % 5 – 50 %
ООО «НПФ «Хеликс»	Да – 50 % Нет – 50 %	Да – 25 % Нет – 75 %	А – 25 % Б – 0 % В – 75 %	А – 0 % Б – 0 % В – 100 %	Да – 50 % Нет – 50 %	1 – 0 % 2 – 0 % 3 – 50 % 4 – 25 % 5 – 25 %
ООО «Газинформсервис»	Да – 50 % Нет – 50 %	Да – 0 % Нет – 100 %	А – 0 % Б – 0 % В – 100 %	А – 100 % Б – 0 % В – 0 %	Да – 25 % Нет – 75 %	1 – 0 % 2 – 0 % 3 – 0 % 4 – 25 % 5 – 75 %
Итого:	**Да – 41,7 % Нет – 58,3 %**	**Да – 8,33 % Нет – 91,67 %**	**А – 16,7 % Б – 16,7 % В – 66,6 %**	**А – 33,33 % Б – 0 % В – 66,67 %**	**Да – 41,7 % Нет – 58,3 %**	**1 – 0 % 2 – 0 % 3 – 25 % 4 – 25 % 5 – 50 %**

Источник: составлено авторами (на основе данных таблицы 1).

Проанализировав полученные результаты, можно сделать вывод, что сотрудники рассматриваемых компаний полностью удовлетворены степенью защиты данных на их рабочих ПК. Большая часть опрошенных ответила, что не встречалась с вирусами на их ПК. Это может быть связано с тем, что сотрудники ответственно подходят к безопасности своего ПК. Кроме того, в ООО «Газинформсервис» существует специализированный отдел, который следит за защитой рабочих ПК. Помимо этого, участники опроса из АО «ЗАСЛОН» и ООО «Газинформсервис» сказали о том, что на свой рабочий ноутбук не могут скачивать какие-либо файлы, чего нельзя сказать об ООО «НПФ«Хеликс». Как было сказано выше, в ООО «Газинформсервис» существует специальный технический отдел, поэтому рабочие компьютеры проходят постоянную диагностику. В АО «ЗАСЛОН» диагностику проводят по необходимости, в то время как в ООО «НПФ«Хеликс» крайне редко, что в дальнейшем может сказаться на кибербезопасности организации. В качестве главных недостатков в защите рабочих ПК участники опроса указали на несвоевременное обновление лицензии и проведение диагностики, также на редкие рассылки правил безопасности от возможных рисков и угроз.

Таким образом, проведенный анализ позволил выделить следующие основные угрозы кибербезопасности в организации:

1) распространение компьютерных вирусов;

2) кража данных с помощью конкурентной разведки или промышленного шпионажа в организации;

3) раскрытие секретной информации в Интернет-ресурсах;

4) непреднамеренные ошибки сотрудников, которые привели к техническим сбоям в работе программного обеспечения (ПО);

5) приостановка деятельности компании в связи с нарушением целостности системы кибербезопасности.

Угрозы кибербезопасности возникают на каждом предприятии, не зависимо от его масштаба и отраслевой принадлежности. А распространение подключенных систем и устройств делает киберпреступность и нарушение работы более заманчивыми для тех, кто намерен совершить преступление.

Выводы

В случае нарушения кибербезопасности предприятия и организации могут испытывать множество негативных (фактических и потенциальных) последствий, в числе которых можно назвать следующие:

1) финансовый ущерб (потеря доходов организации от уменьшения прибыли, хищения денежных средств и пр.);

2) физический ущерб (утечка конфиденциальных данных и информации о клиентах; искажение или удаление содержащих важную информацию файлов; раскрытие коммерческой тайны и пр.);

3) репутационный ущерб (утрата делового имиджа; снижение вероятности роста компании; подрыв общественного мнения);

4) крупные непредвиденные расходы (компании, ставшие объектом атаки, вынуждены платить значительный штраф, который существенно влияет на финансовое состояние бизнеса);

5) потерю клиентов (нарушение безопасности может препятствовать способности организации привлекать и удерживать своих клиентов) [8; 12].

В любом случае все последствия принесут большой финансовый ущерб организации. Например, это может выражаться в упущенной выгоде в результате ухудшения деловой репутации. Также сюда будут непосредственно относиться прямые затраты, связанные с восстановлением предыдущего имиджа и проведением мероприятий по устранению угроз.

Для того чтобы разработать и предложить основные мероприятия по нейтрализации киберугроз на предприятии, необходимо четко понимать, какие именно виды кибератак существуют.

Вредоносные атаки в цифровом мире имеют самые разнообразные формы. Бесчисленные компьютерные вирусы, коды и приложения вредоносных программ ежедневно обрушиваются как на частных лиц, так и на хозяйствующих субъектов. Некоторые из наиболее распространенных и опасных атак используют схожую тактику. Рассмотрим основные из них.

Смишинг – это новейшая техника злоумышленников, направленная на получение доступа к информации. Смишинг приходит через текст, где меньше средств защиты. Для него характерны следующие признаки: видимость того, что текст приходит от надежного источника, ссылки на вредоносные веб-сайты [13].

Фишинг – это получение электронных писем от злоумышленников с целью хищения конфиденциальной информации. Один из самых бесценных советов по кибербезопасности в бизнесе – относиться к любому подозрительному письму с большой осторожностью. При получении сомнительных электронных писем необходимо наводить курсор на гиперссылки (не нажимая на них), чтобы определить, направляют ли они на незнакомую или подозрительную веб-страницу. Если письмо пришло от интернет-провайдера, банка или компании, обслуживающей кредитные карты, то стоит помнить, что эти организации никогда не запрашивают конфиденциальную информацию, например пароль или номер социального страхования [12].

Вредоносное ПО – это коварные атаки, принимающие множество обличий, самое пагубное из которых называется ransomware или программа-вымогатель. При открытии вредоносная программа захватывает важные файлы и блокирует доступ к ним до тех пор, пока жертва не заплатит выкуп за их расшифровку. Ransomware попадает в бизнес-систему, когда ничего не подозревающие пользователи:

1) загружают материалы со взломанного веб-сайта;

2) открывают мошенническое вложение в электронном письме;

3) используют несанкционированный USB-накопитель или другое внешнее медиа-устройство [14].

Социальная инженерия – психологическое манипулирование людьми с целью кражи их личных данных. Киберпреступники используют естественную склонность человека доверять полученному сообщению и/или помогать кому-то, кто нуждается в помощи.

*DDoS-атака (*от англ. *Distributed Denial of Service* – распределенный отказ в обслуживании) – массивная атака на целевую систему организации с целью нарушения ее обслуживания. Это разновидность хакерской атаки, которая перегружает пропускной канал, нарушая работу сервиса (портала, сайта, интернет-магазина etc.). Киберпреступники атакуют сервер компании, перегружая его так, что он значительно замедляется или даже выходит из строя. В этот момент система перестает работать. Это, пожалуй, самая распространенная форма нападения на облачную инфраструктуру и хранилища.

Brute-force – это полный перебор различных комбинаций знаков для атаки с использованием паролей. Этот тип кибератаки происходит, когда хакер использует ПО для определения (и последующей кражи) рабочих паролей [12].

Утечка данных – это преднамеренная или непреднамеренная передача защищенной или конфиденциальной информации ненадежной третьей стороне. Такая атака может нанести ущерб как предприятию в целом, так и его сотрудникам или клиентам.

Вирусы – это программы, способные изменить содержание файлов, привести компьютер к засорению и выполнению негативных действий. Существует множество способов распространения компьютерного вируса: пользователь может открыть вложение в фишинговом письме, запустить исполняемый файл, посетить зараженный веб-сайт или использовать зараженные съемные устройства хранения данных (например, USB-накопитель) [15].

В разработке эффективного плана кибербезопасности должны участвовать не только сотрудники организации, но и руководитель компании. Основные мероприятия, которые необходимо проводить для нейтрализации киберугроз, описаны ниже [16].

1. Регулярно оценивать возможные риски и постоянно обновлять ИТ-системы. Необходимо не реже одного раза в год (по возможности – один раз в полгода) проводить тщательную оценку, уделяя особое внимание выявлению уязвимостей в кибербезопасности. Кроме того, следует проводить плановое техническое обслуживание и регулярно обновлять ПО на всех устройствах компании.

2. Внедрить активную программу обучения для всех сотрудников организации. Безопасность часто ставится под угрозу из-за ошибок или небрежности пользователей. Необходима разработка и реализация программы обучения, чтобы работники понимали, насколько важно сохранять бдительность и быть ответственным при работе с конфиденциальными данными.

3. Создание плана по реагированию на несанкционированное вторжение. Комплексный план реагирования на инциденты, подчеркивающий необходимость немедленного обращения в службу поддержки или специализированный технический отдел, может значительно сократить последствия попытки утечки данных.

Заключение

Киберугрозы носят масштабный характер и имеют большое влияние на деятельность организации. Утечки данных оказывают огромное негативное воздействие на бизнес и часто возникают из-за недостаточно защищенных данных.

Эффективная политика кибербезопасности может помочь обеспечить защиту от прерывания бизнеса и покрыть возможные издержки, понесенные в результате возникновения кибератак.

Кибербезопасность должна быть ключевым приоритетом компании, а ответственность за деятельность по управлению рисками в области кибербезопасности должна быть предусмотрена как внутри организации, так и за ее пределами.

Практическое применение предложенных авторами методов и инструментов предотвращения киберугроз позволит значительно повысить эффективности системы экономической безопасности организации.

Библиографический список

1. Джаферова С.Э. Бухгалтерский учет и кибербезопасность предприятия // Ученые записки Крымского инженерно-педагогического университета. 2022. № 3 (77). С. 36–40. DOI: https://doi.org/10.34771/UZCEPU.2022.77.3.007. EDN: https://www.elibrary.ru/yamhsa.

2. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51–57. DOI: http://doi.org/10.25136/2409-7543.2023.1.40078.

3. Ивасюк О.Н. Современные проблемы противодействия киберпреступности // Вестник экономической безопасности. 2022. № 6. С. 117–120. URL: https://cyberleninka.ru/article/n/sovremennye-problemy-protivodeystviya-kiberprestupnosti/viewer (дата обращения: 17.01.2023).

4. Агаев Р.Ш., Агаев Раф. Ш., Графов А.А. Безопасность информационного сопровождения в системе экономической безопасности // Национальная безопасность и стратегическое планирование. 2022. № 2 (38). С. 98–104. URL: https://futurepubl.ru/ru/storage/viewWindow/97159 (дата обращения: 18.01.2023). DOI: https://doi.org/10.37468/2307-1400-2022-2-98-104. EDN: https://www.elibrary.ru/jlffqv.

5. Лапыгин Д.Ю., Караман К.С. Обеспечение экономической безопасности инструментами информационных технологий // Экономическая безопасность. 2023. Т. 6, № 1. С. 429–442. URL: https://1economic.ru/lib/117577 (дата обращения: 14.01.2023). DOI: https://doi.org/10.18334/ecsec.6.1.117577. EDN: https://www.elibrary.ru/cgpqgk.

6. Дубень А.К. Теоретико-методологические основы информационной безопасности // Национальная безопасность / nota bene. 2023. № 2 (47). С. 48–54. URL: https://nbpublish.com/library_read_article.php?id=40068 (дата обращения: 11.01.2023).

7. Ладжуз М. Кибербезопасность как фактор конкурентоспособности // Kazan Digital Week: сб. мат-лов Междунар. форума (г. Казань, 21–22 сентября 2022 г.). Казань: Научный центр безопасности жизнедеятельности, 2022. С. 299–303. URL: https://elibrary.ru/item.asp?id=50028850. EDN: https://www.elibrary.ru/vylmpt.

8. Tunggal A. What is Cybersecurity Risk? A Thorough Definition // UpGuard: Cybersecurity, 2023. URL: https://www.upguard.com/blog/cybersecurity-risk (дата обращения: 08.01.2023).

9. FBK CyberSecurity: Крупные утечки данных 2022 года в России. URL: https://fbkcs.ru/utechki-dannikh-2022 (дата обращения: 14.01.2023).

10. InfoWatch: Отчет об исследовании утечек информации ограниченного доступа в первой половине 2022 года. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения: 28.01.2023).

11. Positive Technologies: Актуальные киберугрозы: II квартал 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/#id2 (дата обращения: 24.01.2023).

12. Козлов А.В., Клепко К.Ю. Новые проблемы кибербезопасности высших учебных заведений // Университетская наука. 2022. № 2 (14). С. 152–154. URL: https://elibrary.ru/item.asp?id=49811581. EDN: https://www.elibrary.ru/qezazo.

13. Arsenault B. Your Biggest Cybersecurity Risks Could Be Inside Your Organization // Harvard Business Review: Cybersecurity And Digital Privacy, 2023. URL: https://hbr.org/2023/03/your-biggest-cybersecurity-risks-could-be-inside-your-organization (дата обращения: 09.01.2023).

14. Скулаков А.Р., Зенина Е.А. Кибербезопасность корпоративных сетей // Кибербезопасность: технические и правовые аспекты защиты информации: мат-лы межвузовской студенческой научно-практич. конф. (г. Москва, 27 апреля 2022 г.). Москва: МИРЭА, 2022. С. 215–223. URL: https://elibrary.ru/item.asp?id=49250016. EDN: https://www.elibrary.ru/qqdgqs.

15. Сысоенко М.В., Головашова К.Н., Будрина Е.В. Выявление влияния кибербезопасности на решение проблемы утечек больших данных // Скиф. Вопросы студенческой науки. 2023. № 1 (77). С. 80–84. URL: https://elibrary.ru/item.asp?id=50345325. EDN: https://www.elibrary.ru/vtoxgu.

16. Wüest C., Almoula N., Hagen R. How to Build an Organizational Culture that is «Cybersecurity Ready» // World economic forum, 2022. URL: https://www.weforum.org/agenda/2022/08/cybersecurity-ready-organizational-culture-threats (дата обращения: 03.01.2023).

References

1. Dzhaferova S.E. Accounting and cybersecurity of the enterprise. *Scientific Notes of the Crimean Engineering and Pedagogical University*, 2022, no. 3 (77), pp. 36–40. DOI: https://doi.org/10.34771/UZCEPU.2022.77.3.007. EDN: https://www.elibrary.ru/yamhsa. (In Russ.).

2. Duben A.K. Information Security's Place in the National Security System: Actual Problems of Information Law. *Security Issues*, 2023, no. 1, pp. 51–57. DOI: http://doi.org/10.25136/2409-7543.2023.1.40078. (In Russ.).

3. Ivasyuk O.N. Modern problems of countering cybercrime. *Bulletin of economic security*, 2022, no. 6, pp. 117–120. Available at: https://cyberleninka.ru/article/n/sovremennye-problemy-protivodeystviya-kiberprestupnosti/viewer (accessed 17.01.2023) (In Russ.).

4. Agaev R.S., Agaev Raf. S., Grafov A.A. Security of information support in the economic security system. *National Security and Strategic Planning*, 2022, no. 2 (38), pp. 98–104. Available at: https://futurepubl.ru/ru/storage/viewWindow/97159 (accessed 18.01.2023). DOI: http://doi.org/10.37468/2307-1400-2022-2-98-104. EDN: https://www.elibrary.ru/jlffqv. (In Russ.).

5. Lapygin D.Yu., Karaman K.S. Ensuring economic security through information technology tools. *Economic security*, 2023, vol. 6, no. 1, pp. 429–442. Available at: https://1economic.ru/lib/117577 (accessed 14.01.2023). DOI: https://doi.org/10.18334/ecsec.6.1.117577. EDN: https://www.elibrary.ru/cgpqgk. (In Russ.).

6. Duben A.K. Theoretical and Methodological Foundations of Information Security. *National Security*, 2023, no. 2 (47), pp. 48–54. Available at: https://nbpublish.com/library_read_article.php?id=40068 (accessed 11.01.2023) (In Russ.).

7. Lajuz M. Cybersecurity as a factor of competitiveness. In: *Kazan Digital Week: collection of materials of the International forum (Kazan, September 21–22, 2022)*. Kazan: Nauchnyi tsentr bezopasnosti zhiznedeiatel'nosti, 2022, pp. 299–303. Available at: https://elibrary.ru/item.asp?id=50028850. EDN: https://www.elibrary.ru/vylmpt. (In Russ.).

8. Tunggal A. What is Cybersecurity Risk? A Thorough Definition. *UpGuard: Cybersecurity*, 2023. Available at: https://www.upguard.com/blog/cybersecurity-risk (accessed 08.01.2023).

9. FBK Cybersecurity: Group leaks in 2022 in Russia. Available at: https://fbkcs.ru/utechki-dannikh-2022 (accessed 14.01.2023).

10. InfoWatch: Report on the study of restricted information leaks in the first half of 2022. Available at: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (accessed 28.03.2023).

11. Positive technologies: Current cyber threats: II quarter of 2022. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/#id2 (accessed 03.01.2023.

12. Kozlov A.V., Klepko K.Yu. New problems of cybersecurity of higher educational institutions. *University Science*, 2022, no. 2 (14), pp. 152–154. Available at: https://elibrary.ru/item.asp?id=49811581. EDN: https://www.elibrary.ru/qezazo. (In Russ.).

13. Arsenault B. Your Biggest Cybersecurity Risks Could Be Inside Your Organization. *Harvard Business Review: Cybersecurity And Digital Privacy*, 2023. Available at: https://hbr.org/2023/03/your-biggest-cybersecurity-risks-could-be-inside-your-organization (accessed 09.01.2023).

14. Skulakov A.R., Zenina E.A. Cybersecurity of corporate networks. In: *Cybersecurity: technical and legal aspects of information protection: Materials of the interuniversity student research and practical conference (Moscow, April 27, 2022)*. Moscow: MIREA, 2022, pp. 215–223. Available at: https://elibrary.ru/item.asp?id=49250016. EDN: https://www.elibrary.ru/qqdgqs. (In Russ.).

15. Sysoenko M.V., Golovashova K.N., Budrina E.V. Identifying cybersecurity research to address big data leaks. *Skiff. Questions of students science*, 2023, no. 1 (77), pp. 80–84. Available at: https://elibrary.ru/item.asp?id=50345325. EDN: https://www.elibrary.ru/vtoxgu. (In Russ.).

16. Wüest C., Almoula N., Hagen R. How to Build an Organizational Culture that is «Cybersecurity Ready». *World Economic Forum*, 2022. Available at: https://www.weforum.org/agenda/2022/08/cybersecurity-ready-organizational-culture-threats (accessed 03.01.2023).