УДК 330.47

СОВРЕМЕННЫЕ ПОДХОДЫ К АНАЛИЗУ И ОЦЕНКЕ КИБЕРБЕЗОПАСНОСТИ В БИЗНЕСЕ

Кириченко А.О.,
Кубанский государственный аграрный университет имени И. Т. Трубилина, Краснодар,
email: artemolegovickiricenko@gmail.com

Золкин А.Л.,
Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: alzolkin@list.ru

Шамина С.В.,
Южно-Уральский государственный аграрный университет, Челябинск,
email: shamina.troick2@mail.ru

Свердликова Е.А.,
Московский государственный университет имени М.В. Ломоносова, Москва,
email: elena.sverlikova@gmail.com

Аннотация. *Статья посвящена актуальной проблеме кибербезопасности в современной бизнес-сфере. В условиях увеличения числа кибератак и зависимости предприятий от информационных технологий, вопросы обеспечения стабильной работы компаний и защиты конфиденциальных данных становятся критически важными. В статье проводится анализ уровня кибербезопасности бизнес-компаний с использованием метода метрического анализа. Для объективной оценки уровня кибербезопасности предприятия используется взвешенная сумма результатов каждой метрики, умноженной на их вес, отражающий важность каждой метрики. Полученная методология исследования предоставляет организациям инструмент для оценки и улучшения их кибербезопасности, а также адаптируется к конкретным потребностям и специфике работы организации. Кроме того, выбранным методом проводится анализ нескольких компаний. Среди полученных в результате анализа данных определяются различные математические показатели, позволяющие сделать определенные выводы из проведенного исследования: корреляция, дисперсия, математическое ожидание.*

Ключевые слова: кибербезопасность, киберугроза, бизнес, компания, метрика, анализ.

CYBERSECURITY IN BUSINESS: ANALYSIS OF MODERN THREATS

Kirichenko A.O.,
Kuban State Agrarian University named after I.T. Trubilin, Krasnodar,
email: artemolegovickiricenko@gmail.com

Zolkin A.L.,
Povolzhskiy State University of Telecommunications and Informatics (PGUTY), Samara,
email: alzolkin@list.ru

Shamina S.V.,
South Ural State Agrarian University, Chelyabinsk,
email: shamina.troick2@mail.ru

Sverdlikova E.A.,
Lomonosov Moscow State University, Moscow,
email: elena.sverlikova@gmail.com

Abstract. *The article is devoted to the urgent problem of cybersecurity in the modern business sphere. With the increasing number of cyberattacks and the dependence of enterprises on information technology, the issues of ensuring the stable operation of companies and protecting confidential data are becoming critically important. The article analyzes the level of cybersecurity of business companies using the method of metric analysis. To objectively assess the level of cybersecurity of an enterprise, a weighted sum of the results of each metric multiplied by their weight is used, reflecting the importance of each metric. The resulting research methodology provides organizations with a tool for evaluating and improving their cybersecurity, as well as adapting to the specific needs and specifics of the organization's work. In addition, the selected method analyzes several companies. Among the data obtained as a result of the analysis, various mathematical indicators are determined that allow us to draw certain conclusions from the study: correlation, variance, mathematical expectation.*

Keywords: cybersecurity, cyber threat, business, company, metric, analysis

Описание проблемы

Бизнес-сфера, как и любая финансовая или экономическая сфера, в современном мире так или иначе зависит от IT-технологий. Электронные платёжные системы, десятки программ и приложений для автоматизации бизнес-операций, электронная бухгалтерия, учётные системы и т.д. – всё это сегодня является практически неотъемлемой частью любой компании. Однако киберпреступления с целью похищения финансовых ресурсов предприятий и их конфиденциальных данных становятся реальной угрозой для современного бизнеса. Так, согласно исследованию компании MTC RED, количество кибератак в первом полугодии 2023 г. выросло примерно в два раза по сравнению с аналогичным периодом предыдущего года. При этом, наибольшему давлению со стороны хакеров подвергаются IT-бизнес и промышленная сфера.

Актуальность исследования

Исходя из описания проблемы, нетрудно заключить, что вопрос кибербезопасности и обеспечения стабильной работы компаний становится одним из наиболее важных проблем современного бизнеса.

Цель исследования

Цель исследования – разработать методические подходы к оценке кибербезопасности в современном бизнесе, опираясь на исследования российских ученых, определить уровень устойчивости организации к угрозам безопасности информационной структуры.

Обзор литературы

Тема оценки кибербезопасности в современном бизнесе актуальна, поэтому следует рассмотреть мнение исследователей по данному вопросу. К примеру, Астаева А. Ю. в своей работе «ERP-системы и кибербезопасность: как защитить бизнес от угроз» [1] рассматривает ERP-системы как основной инструмент для контроля бизнес-операций и, соответственно, проводит анализ данной технологии выявляя её уязвимости и предлагая решения этих уязвимостей. В числе так называемых «слабых мест» ERP-систем автор называет уязвимости авторизации и аутентифи-

кации, недостатки в сетевом обеспечении данных систем, обработке данных и их возможной неправильной настройке.

Гребешкова И. А., в исследовании «Взаимосвязь бизнеса и кибербезопасности в условиях цифровизации экономики» [3] освещает в общих чертах вопрос о цифровизации современной экономики, а также предлагает различные методы комплексной защиты от кибератак.

В статье «Современные проблемы цифровизации» [4] Зимин А. В. ставит рост угроз кибер-вторжений в деятельность компаний, потерю информации и иные вопросы кибербезопасности в ряд наиболее важных и наиболее остро стоящих в современной экономической повестке дня. Схожего мнения с А. В. Зиминым придерживаются Болдырев М. А. [2], Корнеев М. Н. [5], Кузовлева Н. Ф. [6], Гордеева М. Ю. [7], Сафонова М. Ф. [8]. Все эти исследователи в своих работах объявляют вопросы кибербезопасности, в том числе и по отношению к сферам бизнеса и экономики, чрезвычайно важными и требующими адекватной реакции и эффективных решений. Так, Болдырев М. А. заостряет внимание на том, что инвестирование в развитие сферы кибербезопасности является одной из самых приоритетных задач для любой современной компании. Он неоднократно подчеркивает, что в условиях постоянно эволюционирующей кибер-угрозы и все более сложной и постоянно развивающейся киберпреступности, обеспечение безопасности и конфиденциальности ценных информационных данных компании становится неотъемлемой частью успешного бизнеса. Корнеев М. Н., в свою очередь, делает акцент на большом разнообразии различных кибер-угроз для бизнес-организаций. Он разделяет киберпреступность, кибертерроризм, кибершпионаж, кибератаки, фишинг, DDoS-атаки, атаки программ-вымогателей. Помимо всего прочего, по мнению автора важно помнить и про внутренние угрозы, которые вызывают не меньшую озабоченность у предприятий, поскольку сотрудники организации или подрядчики, имеющие доступ к конфиденциальной информации, намеренно или случайно могут причинить вред.

Кузовлева Н. Ф., классифицирует киберпреступления по иному критерию. Она делит их на киберпреступления экономического, политического, пропагандистского характера. Однако основное место в статье отведено анализу именно правовой базы, регламентирующей вопросы пресечения правонарушений в информационной и экономической среде. Автор анализирует различные юридические документы, положения и регламенты и предлагает собственные меры, которые необходимо предпринять для борьбы с киберпреступностью.

Сафонова М. Ф. в работе исследует различные аспекты вопросов кибербезопасности. Так, автор выделяет несколько этапов работ, выполнением которых можно достигнуть определенного стабильного и высокого уровня в обеспечении киберзащиты. Эти этапы включают в себя:

– аудит, обследование или оценка соответствия внутренним или внешним стандартам и нормативным документам;

– проектирование системы мер кибербезопасности;

– введение средств системы кибербезопасности автоматизированной системы управления технологическим процессом (АСУ ТП);

– сопровождение средств системы кибербезопасности АСУ ТП;

Помимо этого, Сафонова М. Ф. приводит расширенную и подробную статистику по разным параметрам кибербезопасности стран мира, таким как расследо-

ванные и нераскрытые киберприступления, киберугрозы в промышленно развивающихся странах и т.д. По данным этой статистики, Россия входит в тройку стран с самым высоким процентом компьютеров и мобильных устройств, зараженных вредоносным ПО.

Вопросы кибербезопасности рассматривает Филиппов Д. Н. в работе «Проблемы управления ИТ-ресурсами в финансовых организациях» [11]. Среди основных проблем, с которыми сталкиваются финансовые учреждения при управлении своими IT-ресурсами, автор выделяет угрозы кибербезопасности и пробемы конфиденциальности данных.

Кроме того, примечательной является также статья Ибрагимовой Э. С. [9]. Подробно классифицируя основные виды кибер-угроз, автор перечисляет главные методы противодействия атакам со стороны взломщиков: системы обнаружения вторжений (IDS), двухфакторная аутентификация (2FA), резервное копирование и т.д.

Следует упомянуть исследование Пугачевой О. В. «IT-безопасность бизнеса: современные тенденции и направления обеспечения» [10]. В этой работе приводится сравнительная характеристика стран в Глобальном рейтинге кибербезопасности в 2017 г., рассматривается основная причина киберинцидентов, а также даются направления обеспечения информационной безопасности бизнеса. Одним из важных направлений выделяется обучение сотрудников работе с IT-инфраструктурой предприятия и повышение их квалификационных навыков. Согласно мнению автора, «защита не будет эффективной без обучения сотрудников и внедрения политики безопасности. Как показали результаты опроса, значительная часть инцидентов информационной безопасности, приводивших к утечке конфиденциальных данных, происходила по вине сотрудников компании, случайно или намеренно провоцировавших потерю ценной информации».

Методы исследования

В исследовании использован метод метрического анализа, который заключается в выборе подходящих метрик, определении их значимости, анализе и интерпретации полученных результатов для объективной оценки уровня киберзащиты определенной компании.

Определим следующие метрики:

1. Количество инцидентов киберугроз (КИ) – количество инцидентов киберугроз за определенный период времени.

2. Эффективность систем мониторинга (ЭС) – процент обнаруженных и предотвращенных инцидентов относительно общего количества инцидентов.

3. Время восстановления (ВВ) – среднее время, необходимое для восстановления после киберинцидента.

4. Уровень обученности персонала (УО) – процент сотрудников, прошедших обучение по кибербезопасности.

5. Уровень использования многофакторной аутентификации (УИМА) – процент сотрудников и пользователей, использующих многофакторную аутентификацию.

6. Сложность паролей (СП) – уровень сложности паролей, используемых сотрудниками.

7. Уровень защищенности сети (УЗ) – оценка уровня защищенности сетевой инфраструктуры, включая брандмауэры, интранет и другие меры безопасности. Сложносоставная метрика, вычисляется по формуле:

$$УЗС = (ББ \cdot 0,3) + (ОПВ \cdot 0,2) + (МСТ \cdot 0,15) + (АСС \cdot 0,1),$$

где ББ – удельный вес работающих и правильно настроенных брандмауэров, %;

ОПВ – доля успешно обнаруженных и предотвращенных вторжений, %;

МСТ – доля времени, в течение которого происходит мониторинг сетевого трафика, %;

АСС – частота проведения аудита сетевых событий и реагирования на аномалии, ед.

8. Уровень шифрования данных (УШ) – процент данных, передаваемых и хранящихся с использованием шифрования.

9. Уровень обновленности систем (УО) – процент обновленных и обеспеченных патчей систем и приложений.

По данным метрикам производится расчёт общего уровня кибербезопасности компании. Для получения более точного значения необходимо определить вес, т.е. коэффициент важности, каждой метрики. Конечно, конкретная организация имеет возможность редактировать вес конкретной метрики, меняя степень ее важности в зависимости от потребностей и специфики работы, однако в данном исследовании веса распределены исходя из портрета типовой коммерческой компании (рис. 1).

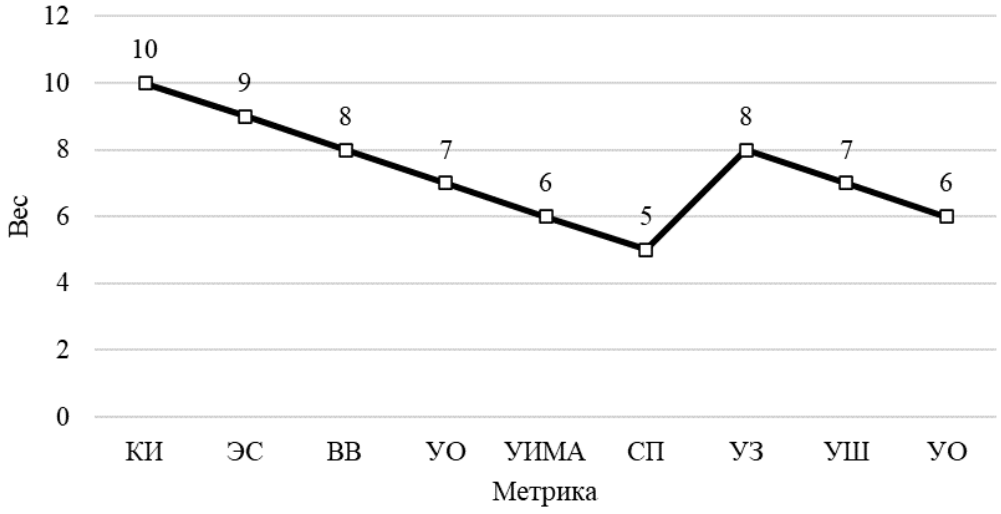

Рис. 1. *Распределение весов по метрикам*

Оценка уровня кибербезопасности (УКБ) исследуемой организации рассчитывается по формуле:

$$УКБ = \frac{\sum(Метрика \cdot Вес)}{\sum Вес}.$$

Таким образом, выбранная методология исследования позволяет получить объективные данные об уровне кибербезопасности анализируемой компании.

Для исследования в статье отобраны 10 компаний агропромышленного комплекса Краснодарского края:

ЗАО «Агрофирма им. Ильича»;
ЗАО имени Мичурина;
АО им. Т. Г. Шевченко;
СПК «Колхоз имени В. И. Ленина»;
ООО «ОПХ им. К. А. Тимирязева»;
ООО «Кубанская крупяная компания»;
ООО «Васюринский МПК»;
ПАО «Племзавод им. В. И. Чапаева»;
ООО «Успенский агропромсоюз»;
ООО «Агротэк».

Для вычисления корреляции между показателями УЗ и УКБ была использована формула корреляции Пирсона:

$$r = \frac{n(\sum XY) - (\sum X) \cdot (\sum Y)}{\sqrt{\left[n\sum X^2 - (\sum X)^2\right] \cdot \left[n\sum Y^2 - (\sum Y)^2\right]}},$$

где n – количество наблюдений,
X – значение УЗ,
Y – значение УКБ.

Для вычисления дисперсии, отражающей стандартное отклонение от среднего значения, используем формулы:

$$M = \frac{\sum_{i=1}^{n} УКБ_i}{n},$$

где n – количество наблюдений,

$$D = \frac{\sum_{i=1}^{n} (УКБ_i - M)^2}{n},$$

где M – значение математического ожидания.

Результаты исследования

В результате исследования были получены показатели эффективности кибербезопасности компаний (табл. 1).

Исходя из данных таблицы 1 видно, что наибольший показатель УКБ имеет компания ЗАО имени Мичурина. Коэффициент корреляции Пирсона между УЗ и УКБ данной организации составляет $r = -0,947$.

Значение коэффициента указывает на сильную отрицательную линейную корреляцию между уровнем защищенности сети и общим уровнем кибербезопасности компании: с увеличением одного показателя, другой уменьшается.

Таблица 1

Основные показатели кибербезопасности компаний

Наименование организации	Показатель УЗ	Показатель УКБ
ЗАО «Агрофирма им. Ильича»	0,55	7,38
ЗАО имени Мичурина	0,58	7,69
АО им. Т. Г. Шевченко	0,54	7,01
СПК «Колхоз имени В. И. Ленина»	0,59	7,27
ООО «ОПХ им. К. А. Тимирязева»	0,58	7,35
ООО «Кубанская крупяная компания»	0,55	7,14
ООО «Васюринский МПК»	0,61	7,43
ПАО «Племзавод им. В. И. Чапаева»	0,59	7,46
ООО «Успенский агропромсоюз»	0,53	7,36
ООО «Агротэк»	0,57	7,27

В рамках настоящей выборки, это может быть связано с ограниченными ресурсами предприятий. Так, вкладываясь в разработку современной и защищенной сети предприятия, руководители упускают разработку и развитие иных не менее важных показателей кибербезопасности – уровню образования сотрудников, безопасности паролей и т.д.

Дисперсия – весьма важный показатель при статистическом анализе данных, показывающая насколько далеко каждое значение отклоняется от среднего и как эти отклонения распределены. Данный показатель помогает нам проводить сравнения, делать выводы о поведении данных, выявлять выбросы и аномалии. Более того, дисперсия является основой для других статистических показателей, таких как стандартное отклонение и коэффициент вариации.

Для полученного набора значений УКБ дисперсия D будет равна 0,0025. Это говорит о крайней сосредоточенности данных возле среднего показателя математического ожидания. Математическое ожидание M равно 7,346. Таким образом, найденные значения говорят о том, что средний уровень кибербезопасности компаний равен 7,346 и разброс показателей относительно этого значения крайне мал – всего 0,0025. Можно сделать вывод о том, что выбранные предприятия АПК имеют очень схожий уровень кибербезопасности и ориентируются на идентичные методы обеспечения целостности корпоративных данных.

Выводы

В данной статье были рассмотрены основные киберугрозы в бизнесе. Современные компании сталкиваются с растущим числом кибератак, похищением финансовых ресурсов и конфиденциальных данных, что делает кибербезопасность одной из наиболее важных проблем современного бизнеса. Авторы научных статей и публикаций на данную тематику выявляют необходимость комплексного подхода к защите от кибератак. Важность инвестирования в развитие сферы кибербезопасности подчеркивается различными исследователями. Отмечается разнообразие угроз, таких как киберпреступность, кибертерроризм, кибершпионаж, что подчеркивает сложность проблемы и необходимость широкого спектра мер по ее решению. В качестве практической части исследования был проведен комплексный анализ уровня кибербезопасности выбранных компаний.

Таким образом, можно заключить, что обеспечение кибербезопасности становится неотъемлемой частью успешного ведения бизнеса. Компании должны активно разрабатывать и внедрять эффективные стратегии по защите от кибер-угроз, а также инвестировать в обучение персонала и развитие технологий, которое позволит им уверенно сопротивляться современным вызовам кибербезопасности и обеспечивать стабильное функционирование в цифровой среде.

Литература

1. Астаева А.Ю. ERP-системы и кибербезопасность: как защитить бизнес от угроз // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, посвященная 170-летию со дня рождения В.Г. Шухова: Сборник докладов, Белгород, 16–17 мая 2023 года. Том Часть 13. Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. С. 36-40.

2. Болдырев М.А. Анализ влияния киберпреступлений на компании, оценка угроз, связанных с кибербезопасностью и разработка стратегий для защиты бизнеса от подобных атак // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: Сборник научных статей. М.: Буки-Веди, 2023. С. 57-60.

3. Гребешкова И.А., Фирстова И.А. Взаимосвязь бизнеса и кибербезопасности в условиях цифровизации экономики // Актуальные вопросы учета и управления в условиях информационной экономики. 2022. № 4. С. 362-367.

4. Зимин А.В. Современные проблемы цифровизации экономики // Проблемы развития современного общества: Сборник научных статей 8-й Всероссийской национальной научно-практической конференции. В 4-х томах, Курск, 19–20 января 2023 года / под редакцией В.М. Кузьминой. Том 1. Курск: Юго-Западный государственный университет, 2023. С. 153-157.

5. Корнеев М.Н., Черпаков И.В. Кибербезопасность и ее значение для защиты экономики от цифровых угроз // Вестник Тульского филиала Финуниверситета. 2023. № 1. С. 342-343.

6. Кузовлева Н.Ф., Гречишкина А.Д. Киберпреступления и кибербезопасность: вопросы теории и практики в Концепции экономической безопасности // Экономика и управление: проблемы, решения. 2024. Т. 3, № 1 (142). С. 25-40. DOI: 10.36871/ek.up.p.r.2024.01.03.004.

7. Гордеева М.Ю. Сравнительный анализ киберпреступности в России и мире, а также способы борьбы с ней // Международный журнал гуманитарных и естественных наук. 2022. № 5-2 (68). С. 303-306. DOI: 10.24412/2500-1000-2022-5-2-303-306.

8. Сафонова М.Ф., Ципляева С.А. Кибербезопасность: проблемы и решения // Естественно-гуманитарные исследования. 2019. № 24 (2). С. 63-68.

9. Ибрагимова Э.С., Сулейманов М.М. Кибербезопасность компаний в эпоху цифровизации экономики // МИЛЛИОНЩИКОВ-2023: Материалы VI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых с международным участием, Грозный, 30–31 мая 2023 года. Грозный: Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова, 2023. С. 80-83. DOI: 10.26200/GSTOU.2023.25.38.012.

10. Пугачева О.В. IT-безопасность бизнеса: современные тенденции и направления обеспечения // Потребительская кооперация. 2017. № 4 (59). С. 34-41.

11. Филиппов Д.Н. Проблемы управления ИТ-ресурсами в финансовых организациях // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XX Международной научно-практической конференции, Москва, 21 апреля 2023 года. М.: Печатный цех, 2023. С. 42-46.