Список использованных источников

1. Баффетт, У. Эссе об инвестициях, корпоративных финансах и управлении компанией / Уоррен Баффетт; сост., авт. Предисл. Лоренс Каннингем; пер. с англ. — М.: Альпина Бизнес Букс, 2005. — 268 с.
2. Государственное регулирование рыночной экономики: Учебник для вузов / Под общей редакцией д-ра экон.наук, проф. В. И. Кушлина, д-ра экон. наук, проф. Н. А. Волгина. — М.: Экономика, 2001. — 735с.
3. Лахметкина, Н. И. Инвестиционная стратегия предприятия: учебное пособие / Н. И. Лахметкина. — М.: КНОРУС, 2006. — 184 с.

УДК 004.056

Э.Р. Шагеев
Казанский инновационный университет им. В.Г. Тимирясова
Казань, Россия

КИБЕРБЕЗОПАСНОСТЬ И БИЗНЕС В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *Реферат рассматривает текущее состояние кибербезопасности в российском бизнесе и предлагает меры для повышения защиты данных и информационных систем. В работе анализируются основные угрозы, рассматриваются технические и организационные аспекты кибербезопасности, а также роль государства и частного сектора. Исследуются новые тенденции и технологии в области кибербезопасности, а также опыт внедрения мер защиты в российских компаниях. Результаты работы подчеркивают необходимость комплексного подхода к защите информации и сотрудничества государства и частного сектора для обеспечения безопасности в цифровой среде.*

E.R. Shageev
Kazan Innovation University named after V.G. Timiryasova
Kazan, Russia

CYBERSECURITY AND BUSINESS IN THE RUSSIAN FEDERATION

Abstract. *The abstract examines the current state of cybersecurity in Russian business and proposes measures to improve the protection of data and information systems. The paper analyzes the main threats, considers technical and organizational aspects of cybersecurity, as well as the role of the government and the private sector. New trends and technologies in cybersecurity are studied, as well as the experience of implementing protection measures in Russian companies. The results of the work emphasize the need for a comprehensive approach to information protection and cooperation between the state and the private sector to ensure security in the digital environment.*

С развитием информационных технологий и интернета бизнес в России сталкивается с новыми вызовами в сфере кибербезопасности. Проникновение интернета в различные сферы деятельности компаний, активное использование облачных сервисов, мобильных приложений и социальных сетей существенно увеличили уязвимость корпоративных данных и систем. Компании всех размеров — от крупных корпораций до малого и среднего бизнеса — становятся мишенями для киберпреступников. Атаки могут быть направлены на кражу конфиденциальной информации, нарушение работы информационных систем, вымогательство и другие формы киберпреступлений.

Текущие вызовы, с которыми сталкиваются компании в России, включают многообразие киберугроз, уязвимость критической инфраструктуры, человеческий фактор и недостаточное финансирование, и ресурсы. Эти угрозы делают необходимость внедрения эффективных мер защиты данных и информационных систем неотъемлемой частью стратегии любой компании. Недостаток внимания к кибербезопасности может привести к серьезным последствиям, включая утрату интеллектуальной собственности, финансовые убытки и нарушение операционной деятельности.

Для успешного противостояния киберугрозам требуется комплексный подход к кибербезопасности, который включает технические, организационные и законодательные меры. Кибербезопасность включает в себя использование современных средств защиты информации, таких как антивирусные программы, фаерволы, системы обнаружения и предотвращения вторжений (IDS/IPS), шифрование данных и регулярное обновление программного обеспечения. Также важно разработать и внедрить внутренние политики безопасности, регулярно проводить аудиты и оценку рисков, обучать сотрудников основам кибербезопасности и создавать планы реагирования на инциденты. Компании должны соответствовать требованиям законодательства РФ в области защиты информации и следовать международным стандартам, таким как ISO/IEC 27001.

Цель данной работы — исследовать текущее состояние

кибербезопасности в бизнесе РФ, выявить основные угрозы и предложить эффективные меры и стратегии для повышения уровня защиты корпоративных данных и информационных систем.

Одной из главных задач является анализ киберугроз, с которыми сталкивается бизнес в России. Это включает исследование различных типов атак, таких как фишинг, вирусы, трояны, DDoS-атаки и программы-вымогатели, а также определение наиболее актуальных угроз для разных секторов экономики. Также необходимо изучить существующие меры и стратегии защиты данных и систем, включая технические решения, организационные меры и методы обеспечения безопасности в облачных средах.

Важной задачей является оценка роли государства и частного сектора в обеспечении кибербезопасности, что включает анализ государственных инициатив и программ поддержки, а также участие частного сектора в этих процессах. Рассмотрение законодательных аспектов кибербезопасности в РФ также является ключевым элементом исследования, охватывающим анализ закона «О персональных данных» и других нормативных актов, а также международных стандартов, таких как ISO/IEC 27001.

Необходимо выявить новые тенденции и технологии в области кибербезопасности, включая использование искусственного интеллекта и машинного обучения для прогнозирования и предотвращения атак, а также разработку новых методов защиты в среде Интернета вещей (IoT).

Также важным аспектом исследования является оценка опыта внедрения различных мер защиты в российских компаниях, чтобы выявить успешные практики и распространенные проблемы. Изучение реальных примеров и кейсов поможет предложить конкретные рекомендации для повышения уровня кибербезопасности в российских компаниях различных размеров и отраслей.

Для успешного противостояния киберугрозам требуется комплексный подход к кибербезопасности, включающий технические, организационные и законодательные меры.

Технические меры играют ключевую роль в обеспечении кибербезопасности. Использование современных средств защиты информации включает в себя антивирусные программы, фаерволы, системы обнаружения и предотвращения вторжений (IDS/IPS), шифрование данных и регулярное обновление программного обеспечения. Антивирусные программы помогают обнаруживать и устранять вредоносное ПО, тогда как фаерволы защищают сеть от несанкционированного доступа. Системы IDS/IPS позволяют

обнаруживать и предотвращать попытки вторжений в реальном времени, а шифрование данных обеспечивает их безопасность при передаче и хранении. Регулярное обновление программного обеспечения необходимо для устранения уязвимостей и защиты от новых видов угроз.

Организационные меры включают разработку и внедрение внутренних политик безопасности, которые определяют правила и процедуры для защиты данных и информационных систем. Важной частью организационных мер является регулярное проведение аудитов и оценка рисков, что позволяет выявлять слабые места в системе безопасности и принимать меры для их устранения. Обучение сотрудников основам кибербезопасности играет ключевую роль в предотвращении инцидентов, связанных с человеческим фактором. Сотрудники должны быть осведомлены о возможных угрозах и обучены правильным действиям при их возникновении. Создание планов реагирования на инциденты позволяет быстро и эффективно реагировать на кибератаки, минимизируя их последствия для компании.

Компании должны соответствовать требованиям законодательства РФ в области защиты информации и следовать международным стандартам, таким как ISO/IEC 27001. Законодательные меры включают соблюдение закона «О персональных данных», который регулирует обработку и защиту персональных данных, а также других нормативных актов, направленных на обеспечение информационной безопасности. Компании должны проводить регулярные проверки на соответствие законодательным требованиям и внедрять необходимые изменения в свои процессы и системы.

Использование инновационных технологий, таких как искусственный интеллект и машинное обучение, может значительно повысить уровень кибербезопасности. Эти технологии позволяют анализировать большие объемы данных и выявлять аномалии, указывающие на потенциальные угрозы. Внедрение методов защиты для Интернета вещей (IoT) также становится все более важным, поскольку количество подключенных устройств продолжает расти. Эти устройства часто имеют слабую защиту, что делает их уязвимыми для атак, и их безопасность необходимо учитывать при разработке общей стратегии кибербезопасности.

Государственные инициативы и программы поддержки играют важную роль в повышении уровня кибербезопасности. Государство может предоставлять ресурсы и поддержку для малого и среднего

бизнеса, который часто не имеет достаточных средств для реализации комплексных мер защиты. Сотрудничество между государством и частным сектором, обмен информацией о угрозах и совместные усилия по разработке и внедрению мер безопасности способствуют созданию безопасной цифровой среды.

В ходе исследования были выявлены новые идеи и результаты, которые имеют важное значение для совершенствования кибербезопасности в бизнесе.

Интеграция искусственного интеллекта и машинного обучения в кибербезопасность предоставляет новые возможности для прогнозирования и предотвращения атак. Эти технологии могут анализировать большие объемы данных и обнаруживать угрозы.

Усиление защиты IoT-устройств является критически важным в контексте роста числа подключенных устройств. Разработка новых методов защиты для IoT-устройств поможет снизить уязвимость этого сегмента информационной инфраструктуры.

Повышение уровня киберграмотности сотрудников через программы обучения в образовательных учреждениях и корпоративных тренингах способствует созданию культуры безопасности и повышению осведомленности о существующих угрозах. Опыт внедрения различных мер кибербезопасности в российских компаниях показывает различные подходы в зависимости от размера и отрасли компании.

Крупные компании активно инвестируют в передовые технологии защиты и создают собственные подразделения по кибербезопасности. Они часто разрабатывают и внедряют собственные политики безопасности и проводят регулярные аудиты для выявления уязвимостей.

Малые и средние компании часто используют доступные решения и государственные программы поддержки для повышения своего уровня кибербезопасности, в связи с ограниченными ресурсами.

Кибербезопасность является критически важным аспектом для успешного ведения бизнеса в цифровую эпоху. Для противостояния киберугрозам необходим комплексный подход, включающий в себя технические, организационные и законодательные меры. Государство и частный сектор должны работать в тесном сотрудничестве для создания безопасной цифровой среды. Постоянное совершенствование технологий, повышение уровня киберграмотности сотрудников и применение передовых методов защиты являются ключевыми факторами в обеспечении безопасности информационных систем и данных.

Список использованных источников

1. https://companies.rbc.ru/news/0x345tuIu0/kakie-trendyi iberbezopasnosti-v-rossii-aktualnyi-v-2024-godu/
2. https://iis.guu.ru/blog/bezopasnost-informacionnih-technologiy/
3. https://russiancouncil.ru/activity/policybriefs/ugrozy-mezhdunarodnoy-informatsionnoy-bezopasnosti-v-epokhu-industrii-4-0/?sphrase_id=141510069

УДК 003.26+004.9

П.П. Урбанович[1,2], **Е.А. Блинова**[1], **А. Керштын**[3], **Н.П. Шутько**[1]
[1]Белорусский государственный технологический университет
Минск, Беларусь
[2]Люблинский Католический университет Яна Павла II
[3]Люблинский технический университет
Люблин, Польша

ЗАЩИТА ПРОГРАММНОГО КОДА НА ОСНОВЕ ДЕТЕКТИРОВАНИЯ И АНАЛИЗА SQL-ИНЪЕКЦИЙ

Аннотация. *Представлены результаты разработки и использования статического анализатора для выявления уязвимостей типа SQL-Injection в исходных кодах мобильных приложений. Условия детектирующего алгоритма проверяются при помощи механизма синтаксических деревьев.*

P.P. Urbanovich[1,2], **E.A. Blinova**[1], **A. Kiersztyn**[3], **N.P. Shutko**[1]
[1]Belarusian State Technological University
Minsk, Belarus
[2]The John Paul II Catholic University of Lublin
[3]Lublin University of Technology
Lublin, Poland

PROTECTION OF SOFTWARE CODE BASED ON DETECTION AND ANALYSIS OF SQL INJECTIONS

Abstract*. The results of the development and use of a static analyzer to identify SQL-Injection vulnerabilities in the source codes of mobile applications are presented. The conditions of the detection algorithm are checked using the mechanism of syntax trees.*

Темпы интеграции мобильных устройств в повседневную жизнь