УДК 004.056.53

ЦИФРОВЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Головко М.В.

профессор, д.э.н., доцент, кафедра институциональной экономики и инвестиционного менеджмента,

ФГБОУ ВО Кубанский ГАУ

Краснодар, Россия

Ларькина Т.М.

обучающаяся экономического факультета,

ФГБОУ ВО Кубанский ГАУ

Краснодар, Россия

Овсепян М.О.

обучающаяся экономического факультета,

ФГБОУ ВО Кубанский ГАУ

Краснодар, Россия

Аннотация. Системы управления информационной безопасностью находят все более широкое применение в ряде секторов новой, глобальной, взаимосвязанной экономики. Их используют производственные и сервисные предприятия, фирмы, предоставляющие услуги информационных технологий и связи, органы государственной власти и органы местного самоуправления. В частности, они используются в случае с преступными группами или как средство обеспечения незаконных сделок. Все эти моменты подтверждают актуальность данного исследования. Целью исследования является рассмотрение различных видов систем информационной безопасности, изучение составляющих элементов, выявление преимуществ каждой из систем. Информационная безопасность и информационные технологии являются самой быстрорастущей отраслью как в России, так и во всем мире. Растущая

компьютеризация как в частном, так и в государственном секторах делает Россию рынком с огромным потенциалом для разработки программного обеспечения, аутсорсинга и услуг безопасности, необходимых для экономического роста и национальной безопасности, что доказывает новизну исследования. Однако быстро развивающийся рынок программного обеспечения России еще не раскрыл весь свой потенциал. В связи с этим авторами статьи анализируются системы безопасности, а также выявляются их лучшие применения в государственных структурах и частных компаниях, что отражено в результате исследования.

Ключевые слова: информационная безопасность, кибербезопасность, инцидент, система безопасности, физическая безопасность, стратегии безопасности, облачная и локальная безопасность.

DIGITAL INFORMATION SECURITY TECHNOLOGIES

Golovko M.V.

Professor, Doctor of Economics, Associate Professor, Department of Institutional Economics and Investment Management,

FGBOU VO Kuban State Agrarian University

Krasnodar, Russia

Larkina T.M.

student of the Faculty of Economics,

FGBOU VO Kuban State Agrarian University

Krasnodar, Russia

Ovsepyan M.O.

student of the Faculty of Economics,

FGBOU VO Kuban State Agrarian University

Krasnodar, Russia

Annotation. Information security management systems are increasingly being used in a number of sectors of the new, global, interconnected economy. They are used by manufacturing and service enterprises, firms providing information technology and communications services, public authorities and local governments. In particular, they are used in the case of criminal groups or as a means of securing illegal transactions. All these points confirm the relevance of this study. The purpose of the study is to consider various types of information security systems, to study the constituent elements, to identify the advantages of each of the systems. Information security and information technology is the fastest growing industry both in Russia and around the world. Increasing computerization in both the private and public sectors makes Russia a market with great potential for software development, outsourcing and security services needed for economic growth and national security, proving the novelty of the study. However, Russia's rapidly developing software market has yet to reach its full potential. In this regard, the authors of the article analyze security systems, and also identify their best applications in government agencies and private companies, which is reflected in the result of the study.
Keywords: information security, cybersecurity, incident, security system, physical security, security strategies, cloud and local security.

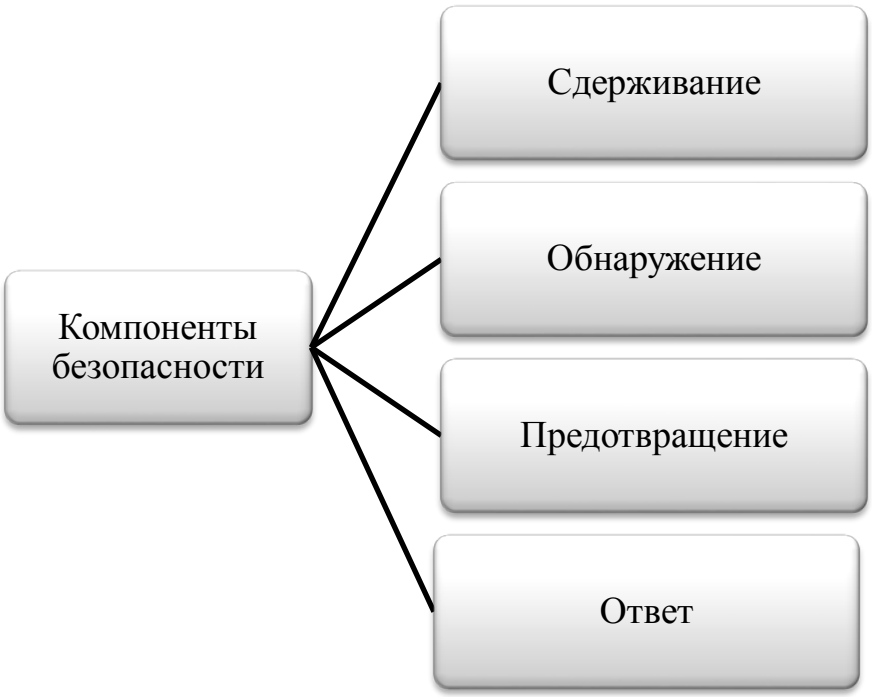
Введение. Новые разработки и идеи продолжают формировать будущее технологий безопасности, а новости о нарушениях безопасности постоянно напоминают о том, насколько важна правильная технология для успеха. Однако выявление и внедрение последних тенденций в области технологий безопасности эффективно только при более глубоком понимании того, что такое технология безопасности и как она работает.

Технологии обеспечения безопасности — это концепции, политики и компоненты, предназначенные для минимизации рисков, выявления уязвимостей и информирования о том, как и когда реагировать на

потенциальные инциденты. Но хорошая безопасность выходит за рамки простой установки системы.

Цель и методы исследования. Цель данной статьи – рассмотреть разнообразные виды систем информационной безопасности, изучить составляющие ее компоненты, а также рассмотреть инциденты информационной безопасности в России. В качестве методов исследования послужили сравнительный анализ, абстрактно-логический, расчётно-конструктивный, графический.

Основная часть. Есть четыре компонента технологии безопасности, которые работают вместе, чтобы создать целостную систему. Данные компоненты представлены на рис. 1.



Источник: авторская разработка

Рис. 1 – Основные компоненты технологии безопасности

Выше были показаны четыре элемента, из которых состоит успешная стратегия. Рассмотрим их более подробно и опишем общие примеры технологий безопасности для каждого из них.

1. Сдерживание. Это стратегии безопасности, используемые в первую очередь для сведения к минимуму риска нарушения безопасности. Это может быть просто физический барьер, такой как забор, ворота или стена. Однако внедрение новейших технологий безопасности также может стать сдерживающим фактором как для физических, так и для кибербезопасности. Камеры видеонаблюдения, коммерческие дверные замки с поддержкой IoT и защита паролем — все это примеры технологий безопасности, которые могут удержать людей от попыток получить несанкционированный доступ к пространству или информации.

2. Обнаружение – это возможность быстрого выявления инцидента, ключ к минимизации нанесенного ущерба. В связи с этим технологии безопасности, такие как контроль доступа, который может уведомить команды о взломе двери, системы сигнализации и мониторинг сети в режиме реального времени, необходимы для полной стратегии безопасности.

3. Предотвращение. В отличие от сдерживания, этот компонент предназначен для задержки или замедления развития нарушения или вторжения. Примеры технологий безопасности, попадающие в эту категорию, включают несколько форм контроля доступа, шифрование данных, многофакторную аутентификацию, которая является одной из основных тенденций кибербезопасности.

4. Ответ – это применение продуктов технологий безопасности, например, блокировка зданий, удаленный доступ и средства управления, а также возможность отправки прямых видеопотоков службам экстренного реагирования.

Важность информационной безопасности в организациях невозможно переоценить [1]. Крайне важно, чтобы компании предприняли необходимые шаги для защиты своей приоритетной информации от утечек данных, несанкционированного доступа и других разрушительных угроз безопасности данных для бизнеса и данных потребителей.

По данным компании RTM Group, которая проводила оценку на основе возбужденных уголовных дел, связанных с использованием информационных технологий, в 2021 г. в России зарегистрировано около 518 тысячи киберпреступлений, что на 1,4% больше, чем в 2020 г. и в 1,8 раза больше аналогичного показателя 2019 г.

Как правило, технологии безопасности делятся на две основные категории: физическая безопасность и кибербезопасность, отличительные особенности которых заключены в конструкции и вариантах использования этих типов.

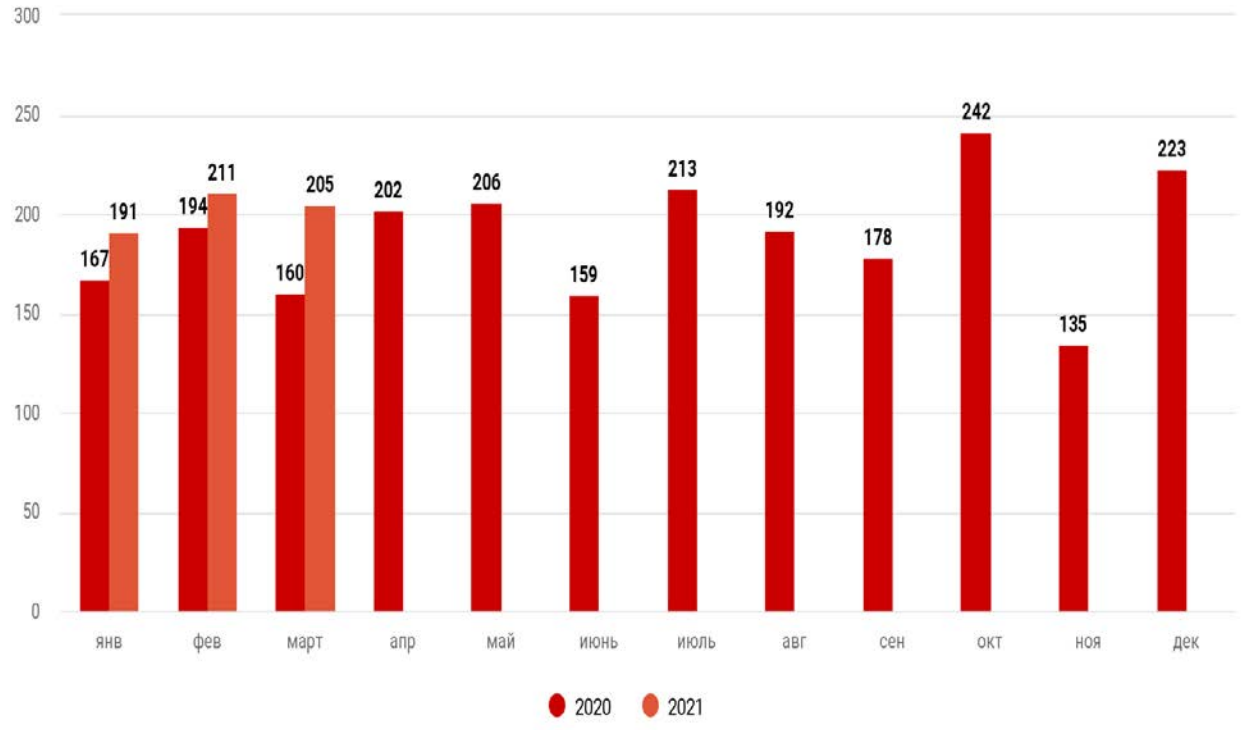
Физическая безопасность — это методы защиты от физических вторжений или действий в пространстве, включая инструменты и технологии, используемые для мониторинга физических пространств и действий людей в этой среде. Тремя основными компонентами являются контроль доступа, наблюдение и тестирование. Некоторые организации неохотно инвестируют в новейшие технологии безопасности для этого сектора, но физическая безопасность также играет ключевую роль в защите данных и информации. Благодаря последним инновациям и тенденциям в области облачной безопасности технология физической безопасности становится все умнее, с новыми возможностями для подключения к другим системам и улучшения реагирования на инциденты (ГОСТ Р ИСО/МЭК 18044), которые представлены на рис. 2. Эта функциональная совместимость является одной из причин, по которой тенденции физической безопасности в 2022 г. указывают на технологии, использующие облачное программное обеспечение и искусственный интеллект.

Источник: авторская разработка

Рис. 2 – Инциденты информационной безопасности

Наглядным примером инцидента информационной безопасности является событие августа 2022 года: за месяц, когда бывшего президента США обвинили в незаконном присвоении секретных правительственных документов, также произошло множество злонамеренных инсайдеров, скомпрометировавших системы своего работодателя. Между тем, бастион безопасности паролей, LastPass, объявил, что: «Наши системы были взломаны, хотя организация уверена, что данные клиентов остаются в безопасности». Всего в августе в США выявили 112 публично раскрытых инцидентов безопасности, в результате которых было скомпрометировано 97 456 345 записей. Исходя из этого, можно сказать, что август 2022 года стал уроком осторожности при предоставлении конфиденциальной информации.

Рассмотрим инциденты информационной безопасности в России за 2020-2021 г. на рис. 3.



Источник: авторская разработка

Рис. 3 – Количество инцидентов информационной безопасности в РФ, 2020-2021 гг. (по месяцам)

Анализируя сводные данные, представленные на рисунке 3, можно сделать следующие выводы: количество инцидентов в I квартале 2021 года в сравнении с аналогичным периодом 2020 года увеличилось на 17%, а относительно IV квартала 2020 прирост составил 1,2%. На организации были направлены 88% атак. Исходя из материалов Positive Technologies, ведущего разработчика решений для информационной безопасности, можно процитировать следующую информацию: «Чаще всего злоумышленники атаковали госучреждения, промышленные компании и организации в сфере науки и образования. Основным мотивом в атаках как на организации, так и на частных лиц остается получение данных[5]. Главными целями злоумышленников являются персональные и учетные данные, а при атаках на организации к ним добавляется еще и коммерческая тайна».

Говоря в широком смысле о защите цифровых активов, кибербезопасность относится к стратегиям, которые защищают информацию, данные и сети. Кибербезопасность, а также ее подмножества информационной безопасности и безопасности информационных технологий, становятся все более заметными среди тенденций индустрии безопасности.

Недавние новости о нарушениях безопасности часто включают истории о хакерах, получающих доступ к конфиденциальной информации путем обхода средств контроля кибербезопасности или компрометации систем безопасности информационных технологий. Поскольку этот тип технологий используется для защиты цифровых активов как от внутренних, так и от внешних угроз, каждая организация должна знать последние тенденции в области кибербезопасности, если они хотят не стать жертвой. Знание различных типов систем кибербезопасности является ключом к внедрению передового опыта.

На самом деле, лучшие стратегии безопасности объединяют физические и кибернетические ресурсы, что также известно, как конвергенция безопасности. Понимание различий между этими продуктами технологий безопасности, а также того, как они взаимодействуют друг с другом, помогает компаниям лучше подготовиться к будущему безопасности.

Выбор правильной системы безопасности является важным решением и часто требует крупных инвестиций для организации любого размера. Существует два типа систем с ключевыми отличиями: облачные и локальные решения. Рассмотрим их более подробно и выделим преимущества.

Основным отличием является то, где эти системы управляются. Локальная технология безопасности работает на локально управляемых серверах на строительной площадке и рассматривается как более традиционный или «устаревший» вариант. В облачных системах серверы управляются третьей стороной, а локальные данные синхронизируются через облако [2]. Большинство поставщиков технологий облачной безопасности

используют Amazon Web Services, Google Cloud и Microsoft Azure для управления своими серверами.

Причины, по которым стоит выбрать локальные системы безопасности:

– локально используется программное обеспечение «толстого клиента», которое предлагает более широкие возможности настройки;

– программное обеспечение для управления может быть основано на браузере или привязано к конкретной локальной рабочей станции;

– хороший вариант для сред с высоким уровнем безопасности со строгими требованиями политики или соответствия;

– установка, обслуживание и обновления выполняются обученным IT-специалистом на месте, который знает конкретную систему;

– совместимость с существующими локальными системами безопасности.

Причины выбрать облачные системы безопасности:

– устраняет необходимость вкладывать средства в локальное оборудование и управление IT;

– простое масштабирование благодаря полностью удаленным возможностям управления и отсутствию необходимости установки серверного оборудования на месте;

– обновления программного обеспечения автоматически устанавливаются через облако;

– новые возможности и функции легче и быстрее развертываются на всех сайтах;

– избыточность, встроенная в крупные центры обработки данных, повышает надежность облачной системы;

– технология облачной безопасности часто строится на открытых стандартах для легкой интеграции с другими системами.

Если в организации уже есть локальная система безопасности, но ей также нужен доступ к некоторым возможностям облачной системы, то существуют облачные системы безопасности, обратно совместимые с устаревшими технологиями.

В гибридной модели организации могут сохранить свои первоначальные инвестиции в локальные серверы и обновить пограничные устройства до облачных технологий. Например, организация, которая хочет сохранить свое исходное локальное оборудование ACU, может обновить свои дверные считыватели с помощью поставщика облачной системы контроля доступа, такого как Openpath, что позволит им воспользоваться преимуществами беспроблемных мобильных учетных данных и удаленного управления без необходимости переделывать или менять всю систему.

Результаты и заключения. Таким образом, можно сделать вывод, что будущее технологий безопасности будет в значительной степени зависеть от новых способов централизации данных и автоматизации операций. Облачные системы, программное обеспечение на основе искусственного интеллекта и более надежные соединения IoT — все это ключ к навигации в новом ландшафте безопасности. Поскольку организации ищут новые способы сделать рабочие места более эффективными и поддерживают устойчивую гибридную модель работы, правильная технология безопасности будет играть решающую роль в способности быстро адаптироваться к потребностям арендаторов и сотрудников, а также защищать данные и информацию от множество новых угроз кибербезопасности.

Библиографический список:

1. Nuriev, B. D. Information technology industry state support as a key problem of ensuring the national security of the Russian Federation / B. D. Nuriev, S. V. Pospelov // Upravlenie. – 2022. – Vol. 10. – No 3. – P. 67-71.

2. Головко М.В., Анцибор А.В., Рогачева Ж.С. К вопросу о влиянии цифровых технологий на экономическую безопасность предприятий / В книге: Безопасность ядерной энергетики. Тезисы докладов XVII Международной научно-практической конференции. Волгодонск, 2021. С. 66-69.

3. Ефремова Е.Н., Пардаева А.Д. Применение современных информационных технологий при обеспечении уровня безопасности // Поиск (Волгоград). 2021. № 1 (11). С. 117-121.

4. Постникова М.С. Современные технологии обеспечения информационной безопасности // Тенденции развития науки и образования. 2021. № 72-1. С. 98-100.

5. Смирнов А.М. Тренды, угрозы, технологии защиты, статистика по информационной безопасности 2022 // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2022. № 1. С. 27-29.

Оригинальность 81%