8. Попова И. Н., Сергеева Т. Л. Импортозамещение в современной России: проблемы и перспективы. 2022. № 2(43). С. 73–84. / [Электронный ресурс]. – Режим доступа: URL: https://www.elibrary.ru/item.asp?id=49244513. Дата обращения: 15.04.2024

9. Селюков М.В. Позиционирование российских производителей на мировом рынке продукции АПК: проблемы и перспективы / М.В. Селюков, Н.П. Шалыгина // Экономика. Информатика. – 2023. – 50(1). – С. 5–17.

10. Селюков М.В. Развитие внешнеторгового потенциала России как фактор обеспечения экономической безопасности государства / М.В. Селюков, Н.П. Шалыгина // Экономика. Информатика. – 2024. – 51(1). – С. 93–106.

УДК 338

СОВРЕМЕННЫЙ РЫНОК СЕТЕВОЙ БЕЗОПАСНОСТИ

Д.А. Кузнецов
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет

В статье проведено исследование содержания сетевой безопасности. Обобщены основные тенденции рынка сетевой безопасности на современном этапе развития.

Ключевые слова: *сетевая безопасность, информация, рынок сетевой безопасности, кибератака.*

THE MODERN NETWORK SECURITY MARKET

D.A. Kuznetsov
Belgorod, Russia
Belgorod State National Research University

The article examines the content of network security. The main trends of the network security market at the current stage of development are summarized.

Keywords: *network security, information, network security market, cyber attack.*

В условиях современного информационного общества вопрос сетевой безопасности стоит особенно остро, поскольку современные реалии развития информационных отношений подразумевают широкое использование и высокую ценность информации, а значит огромный поток передаваемой информации всегда будет подвергаться недобросовестной деятельности.

В 2024 году ситуация в сфере сетевой безопасности продолжает ухудшаться. Ландшафт угроз развивается со стремительной скоростью, и компании вынуждены быстро адаптироваться. Для обеспечения безопасности бизнеса или государственной структуры от угроз, необходимо непрерывно изучать тему сетевой безопасности и быть в курсе основных прогнозов.

В рамках изучения вопроса темы следует дать определения основным терминам, характерным для данной отрасли.

Сетевая безопасность – комплекс мер, предпринимаемых с целью обеспечения защиты сети и данных. Сетевая безопасность представляет собой отрасль кибербезопасности, сочетающая различные технологии и процессы, направленные на защиту сетей и устройств от кибератак или несанкционированного доступа.

Сетевая безопасность – это набор политик и требований, предъявляемых к инфраструктуре сети организаций для предотвращения и мониторинга попыток

несанкционированного доступа, модификации информации, возможного отказа работы всей компьютерной сети и других сетевых ресурсов.

Для обеспечения сетевой безопасности используются различные программные и аппаратные средства, такие как: прокси-серверы, межсетевые экраны, средства обнаружения и предотвращения вторжений (IPS/IDS), антивирусы, антиспам, антифишинг, средства мониторинга сети, средства для защиты от целевых атак, средства безопасности беспроводных сетей, VPN.

Использование указанных средств обеспечивает защиту внутренней сети от несанкционированного доступа, обеспечивает безопасное подключение устройств к внешней сети и возможность осуществления удаленного доступа, а также мониторинг и контроль приложений, имеющих доступ к персональным данным.

Таким образом, объектом деятельности участников кибербезопасности является информация. В рамках вопроса следует определить фундаментальные свойства информации:

Конфиденциальность – уверенность владельца информации в отсутствии прямой или косвенной возможности других участников рынка получить доступ к данной информации. В качестве примера следует привести тайное послание, которое вы передали другому человеку и рассчитываете на то, что информацию и текст послания получит и узнает исключительно получатель послания.

2. Целостность – свойство информации, предполагающее, что информация не будет изменена без ведома автора. Например, вы отправили объем информации получателю. Вы рассчитываете на то, что получателю достанется информация в той форме, виде и объеме, в котором она была изначально отправлена.

3. Доступность – свойство информации, отвечающее за возможность хранения вами информации в любом из доступных форматов и возможность при необходимости использовать эти данные. В качестве примера следует привести оставленные пароли от ваших банковских ячеек в облачном хранилище.

Таким образом были определены основные свойства информации. В современном мире наибольшая часть взаимодействий происходит по средствам использования ИТ-инфраструктуры. Этим фактом обеспечена необходимость поддержания и применения ряда мер по сохранению и поддержанию защищенности передачи данных.

Сетевая безопасность является ключевым и одновременно базовым направлением в киберзащите современной организации. Именно средства защиты сетевого периметра являются одной из первых преград на пути злоумышленника.

Основные тенденции рынка сетевой безопасности сегодня:

Растет внимание к безопасности цепочек поставок ПО. Это включает в себя проверку происхождения компонентов и оценку политик безопасности поставщиков.

Тренд на отказ от паролей в пользу беспарольной аутентификации. Такие стандарты, как passkeys, используют биометрические факторы и обеспечивают более высокий уровень безопасности.

Кибератаки становятся инструментом геополитических конфликтов. «Лаборатория Касперского» в октябре 2023 года заявила о двух волнах вредоносных рассылок в учреждения государственного и индустриального секторов России. Ранее в августе Лаборатория выявила серии сложных целевых кибератак на промышленные предприятия в Восточной Европе с использованием новых версий вредоносного ПО. Такие атаки часто остаются незамеченными до тех пор, пока ущерб не станет очевидным.

Организации стали активно использовать облачные хранилища с целью хранения данных в надежном месте. Однако, надежность облачных хранилищ также находится под вопросом, поскольку злоумышленники разрабатывают все новое ПО с целью кражи данных.

Отдельно следует выделить факт высокого процента использования иностранного ПО и сервисов защиты данных (49%), таких как: VPN/СКЗИ (сервис, обеспечивающий возможность безопасного подключения к сети через удаленную точку доступа), CASB

(сервис, способствующий безопасной передаче данных в облачные хранилища, WAF (сервис для обнаружения попыток взлома). Тенденция к снижению объема потребления иностранного ПО российским рынком наблюдается уже сегодня. Однако, многие сервисы на сегодняшний день отечественный производитель еще не научился интерпретировать. В 2022 году спрос на решения по этому направлению вырос еще больше, особенно в связи с участившимися атаками.

В случае обнаружения угроз в трафике специалисты информационной безопасности заказчика теперь получают автоматические уведомления, что ускорило реакцию на инциденты кибербезопасности.

В целом, по мнению респондентов, на российском рынке решений ИБ для сетевой безопасности нет критичных сложностей в связи с уходом иностранных вендоров, почти половина опрошенных (44%) представителей российских компаний используют отечественные решения, на которые они перешли за прошедший год, либо использовали их изначально.

Российский рынок сетевой безопасности остается импортозависимым. Почти в половине (49%) российских компаний для обеспечения сетевой безопасности продолжают применять зарубежные решения. При этом отечественные решения в большинстве своем находятся на одном уровне с импортными разработками по степени зрелости (53%). По мнению респондентов, полностью аналогичны зарубежным разработкам отечественные системы анализа трафика (NTA) – так считает 58%, во многом уступают зарубежным наработкам – межсетевые экраны (FW, NGFW) – 44%. На шаг впереди зарубежных решений 21% респондентов отметили российские Web Application Firewall (WAF).

В заключение следует дополнительно акцентировать внимание на степени важности обеспечения сетевой безопасности в современных реалиях, поскольку основной способ обмена и передачи данных сегодня представляет собой ИТ-инфраструктура.

Касаемо рынка сетевой безопасности в России: на сегодняшний день существует большой объем возможностей для продавцов данного рынка из-за ухода крупных представителей иностранных ИТ-компаний. У российских разработчиков и программистов есть все шансы полностью заменить иностранные ИТ-продукты на рынке, предложив более устойчивые и конкурентноспособные платформы для бизнеса. Риски, связанные с параллельным импортом и ростом ИТ-пиратства также способствуют процветанию рынка сетевой безопасности в странах СНГ.

ЛИТЕРАТУРА

1. Владыка М.В., Чистникова И.В., Бурдинская Д.М., Тикунов В.И. Методический базис оценки продовольственной безопасности регионов // АПК: экономика, управление. – 2023. – № 8. – С. 3-10.

2. Чистникова И.В., Дружникова Е.П., Добродомова Т.Н. Стратегическое управление пространственным развитием территорий // Естественно-гуманитарные исследования. – 2023. – № 6 (50). – С. 508-511.

3. Чистникова И.В. Территориальное позиционирование как элемент стратегического управления регионом // Экономико-управленческий конгресс. Сборник статей по материалам Международного научно-практического мероприятия НИУ «БелГУ». Отв. редактор: В.М. Захаров. Белгород, 2022. –С. 329-332.