DOI 10.37882/2223-2966.2025.04.34

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ КОНЦЕПЦИИ BYOD

INFORMATION SECURITY FOR THE BYOD CONCEPT

V. Prokhorov
D. Maznin

Summary. This article addresses the issue of cyber security in organizations that allow employees to use personal devices to perform work tasks. The very use of personal devices by employees is driven by the desire of organizations to significantly reduce financial costs for creating new and maintaining existing automated workplaces. However, this desire of organizations raises the question of trust in employees and trust in their personal devices. Therefore, the result of this article is the considered ways of ensuring cyber security in organizations using personal devices of employees. So, this article will consider a way to collect information about the activities of an employee and his device on the organization's network, a way to ensure controlled access of an employee (device) to the organization's network, and a way to manage an employee's personal device. Special attention is paid to the concept of «zero trust», in which the cyber security system should be based on its worst-case assumptions. The use of such a concept is due to the constant distrust of the security of the employee's personal device and himself. To provide such results, the method of analyzing and studying scientific and technical literature, as well as the method of critical evaluation of the methods presented in the article, was used.

Keywords: cyber security, zero trust, BYOD.

Прохоров Виталий Андреевич
Магнитогорский государственный технический университет имени Г.И. Носова
UnknowParrot@yandex.ru
Мазнин Дмитрий Николаевич
Доцент, начальник отдела,
Магнитогорский государственный технический университет имени Г.И. Носова
maznin@inbox.ru

Аннотация. Данная статья затрагивает проблему обеспечения информационной безопасности в организациях, разрешающих применение личных устройств сотрудников для выполнения рабочих задач. Само применение личных устройств сотрудников обусловлено желанием организаций существенно снизить финансовые расходы на создание новых и поддержание существующих автоматизированных рабочих мест. Однако такое желание организаций порождает вопрос об доверии к сотрудникам и об доверии к их личным устройствам. Поэтому основным результатом данной статьи являются рассмотренные способы обеспечения информационной безопасности в организациях, применяющих личные устройства сотрудников. Так, в данной статье будет рассмотрен способ сбора информации о деятельности сотрудника и его устройства в сети организации, способ осуществления контролируемого доступа сотрудника (устройства) в сеть организации и способ управления личным устройством сотрудника. Особое внимание при таком рассмотрение уделяется концепции «нулевого доверия», при которой система информационной безопасности должна строиться из расчета своих худших предположений. Использование такой концепции обусловлено постоянному недоверию к безопасности личного устройства сотрудника и его самого. Для предоставления таких результатов использовался метод анализа и изучения научной и технической литературы, а также метод критической оценки представленных в статье способов.

Ключевые слова: информационная безопасность, нулевое доверие, BYOD.

Введение

В настоящее время во многих организациях набирает популярность использование концепции «принеси свое личное устройство» (bring your own device — BYOD). Данная концепция предлагает сотрудникам организаций использовать свои личные устройства: смартфоны, планшеты, нетбуки, ноутбуки и многие другие устройства — для выполнения рабочих задач.

Использование личных устройств сотрудников позволяет организациям существенно сократить расходы на покупку современного оборудования и соответствующего оборудованию лицензируемого программного обеспечения. Кроме того, личные устройства сотрудников зачастую оказываются мощнее купленных организацией устройств и оказываются для сотрудников более удобными и привычными для использования в рабочих целях.

Основным препятствующим фактором роста популярности концепции BYOD может послужить множество рисков, связанных с информационной безопасностью организации [1]. Данный фактор особенно выделяется при использовании концепции «нулевого доверия» (zero trust), когда злоумышленником может являться сам владелец личного устройства, то есть сам сотрудник организации [2, 3].

Поэтому основной целью данной работы является изучение и анализ существующих решений по обеспечению информационной безопасности в организациях, которые могут быть применены с концепцией BYOD. В качестве дополнительной цели для данной работы яв-

ляется определение оптимального решения среди проанализированных.

Литературный обзор

Теоретической основой данного исследования послужили недавние работы Терещенко Г.В., Новиковой Ю.А., Попова Д.А., Вартаняна А.А., и многих других авторов прямо или косвенно затрагивающие проблемы информационной безопасности в концепции BYOD [1, 4, 5].

Ключевую особенность в данную работу вносит рассмотрение существующих способов обеспечения информационной безопасности для концепции BYOD с различных сторон. Так, дополнительно были рассмотрены работы Кравец А.Г., Цыбенко О.С. и многих других авторов, посвящённые сетевой безопасности, а также работы Кошиев К.Х., Боготов И.М., Агаджанян Э.Ю. и многих других авторов посещенные концепции «нулевого доверия» [2, 3, 6, 7, 8, 9, 10].

Материалы и методы

Для проведения анализа существующих решений по обеспечению информационной безопасности в рамках концепции BYOD использовались следующие методы:

- Метод анализа и изучения научной и технической литературы, посвящённой вопросам обеспечения информационной безопасности в организациях. В рамках данного метода были определены основные решения обеспечения информационной безопасности для концепции BYOD.
- Метод критического анализа существующих решений обеспечения информационной безопасности в рамках концепции BYOD. Дополнительно к данному методу была произведена оценка применимости найденных решений в рамках концепции «Нулевого доверия».

Для определения оптимального решения использовался метод оценки представленных решений по сложности их внедрения в организации, а также по возможному охвату их применения в различных организациях.

Результаты

Перед определением результатов анализа существующих решений обеспечения информационной безопасности в рамках концепции BYOD стоит определить основные принципы концепции «нулевого доверия»:

- Субъекты в информационной системе организации должны иметь безопасный и подтвержденный контролируемый доступ ко всем информационным ресурсам.
- Субъекты в информационной системе организации должны иметь наименьшее количество привилегий к объектам информационной системы организации.
- Действия субъектов в информационной системе организации должны отслеживаться и анализироваться.

Учитывая данную информацию первой группой решений, являются системы мониторинга за информацией, генерируемой личными устройствами сотрудников [5, 7]. Данные системы в рамках концепции «нулевого доверия» отслеживают и анализируют действия сотрудников в информационной системе организации.

В рамках концепции BYOD системы мониторинга можно разделить на несколько больших групп:

- Системы мониторинга, требующие прямого содействия владельца личного устройства. Так, для работы данных систем необходимо, чтобы личные устройства сотрудника генерировали и предоставляли определенные данные на соответствующий удалённый сервер внутри организации.

Ярким примером такой системы может послужить технология централизованного сбора логов, когда сотруднику необходимо вручную настроить отправку логов со своей операционной системы на удаленный сервер.

- Системы мониторинга, не требующие содействия владельца личного устройства. Так, для работы данных систем необходимо осуществлять сбор всего сетевого трафика, циркулирующего между различными сетевыми устройствами в информационной системе организации.

Главным плюсом первого подхода является возможность получения любого вида информации с личного устройства сотрудника, однако такие системы в чистом виде нигде не используются из-за невозможности быстрого реагирования за фактом прекращения выдачи информации с личного устройства сотрудника.

Главным плюсом второго подхода является возможность для организации постоянного сбора информации о сетевой активности сотрудников в организации, однако такие системы не предоставляют данные хранящиеся и использующиеся только внутри личного устройства.

Иной группой решений являются системы контроля сетевого доступа сотрудников. В рамках концепции «нулевого доверия» данные системы осуществляют контролируемый доступ ко всем информационным ресурсам организации путем выдачи определенных сетевых доступов согласно заранее прописанным сотрудникам привилегиям.

Ярким примером системы контроля сетевого доступа является группа технических решений, основанных на стандарте «IEEE 802.1X». Так, в случае использования данного стандарта пользователь сначала проходит

аутентификацию, авторизацию или идентификацию и только потом получает соответствующий ему сетевой доступ в сети [9].

Главным плюсом контроля сетевого доступа является возможность организации постоянной проверки соответствия сотрудников, а также возможность интеграции с иными информационными системами. Главным минусом данной технологии является довольно ограниченный базовый функционал у большинства имеющихся систем.

Третьей группой решений являются системы универсального управления конечными устройствами и их возможные отдельные составляющие в виде систем управления мобильностью предприятия, систем управления мобильными приложениями и систем управления мобильными устройствами [10]. Данные системы в концепции «нулевого доверия» осуществляют контролируемый доступ сотрудников к информационным ресурсам организации путем полного контроля его конечного устройства.

Главным преимуществом таких решений является полный контроль действий сотрудника, возможность навязывания политик организации и программных средств по защите информации без согласия сотрудника, а также возможность удаления конфиденциальной информации в случае утери личных устройств. Однако такое решение характеризуется сложностью внедрения и возможным сопротивлением сотрудников из-за факта постоянного управления и слежения за его личным устройством.

Обсуждение

Оптимальным решением среди проанализированных по охвату применения и довольно низкой сложности внедрения в любые организации являются системы контроля сетевого доступа. Так, в современном мире большинство организаций уже имеют беспроводное подключение в интернет через определенные системы управления доступом. Зачастую такие системы работаю на протоколе RADIUS требующих лишь базовых сетевых знаний для настройки.

В дополнение к этому внедрение такого решения не требует значительного изменения сетевой инфраструктуры, а предоставляемые возможности настройке дают возможность легкой интеграции с другими системами. Например, зачастую такие системы дают возможность добавление пользовательских программных модулей, что с включенной функцией предоставления гостевого доступа в изолированный сегмент информационной системы дает безграничные возможности по интеграции с другими системами.

Например, подобные системы можно интегрировать с системами мониторинга за информацией, где первые будут постоянно подтверждать факт работы последних на личных устройствах сотрудников, тем самым убирая основные проблемы последних в концепции BYOD.

Заключение

В рамках данной работы были проанализированные различные решения по обеспечению информационной безопасности в организациях, которые могут быть применены с концепцией BYOD. Также в ходе работы было определено оптимальное решение среди проанализированных.

В заключении также стоит добавить, что внедрение любого решения, связанного с информационной безопасностью организации, должно добавляться соответствующими политиками по безопасности в организации, иначе выгода внедрения любых решений стремится к нулю.

ЛИТЕРАТУРА

1. Терещенко Г.В., Новикова Ю.А., Попов Д.А. Преимущества и недостатки использования личных мобильных устройств в финансовых организациях // Инженерный вестник Дона. — 2023. — №3(99). — С. 14–29.
2. Сааков В.В., Кошиев К.Х., Боготов И.М., Агаджанян Э.Ю. Концепция Zero Trust или что такое принцип нулевого доверия // Наука и образование: сохраняя прошлое, создаём будущее: сборник статей XXXIX Международной научно-практической конференции. — Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. — С. 52–54.
3. Кирильчук С.П., Аблитаров Э.Р. Архитектура нулевого доверия как инновационный инструмент в системе обеспечения защиты корпоративной информации // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. — 2024. — №3. — С. 45–57.
4. Вартанян А.А. Угрозы и атаки сетевой безопасности // E-Scio. — 2023. — №4(79). — С. 15–20.
5. Цымбал Ф.А. Управление инцидентами безопасности и событиями (SIEM) // Столыпинский вестник. — 2022. — №4
6. Кравец А.Г., Сальникова Н.А. Метод назначения прав доступа к приложениям в корпоративной мобильной сети // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. — 2023. — №1. — С. 71–82.
7. Цыбенко О.С. Технологии и решения сетевой безопасности // E-Scio. — 2023. — №4(79). — С. 100–105.
8. Хусаинова М.К. Сетевая безопасность и мониторинг // ReFocus. — 2022. — № 4. — С. 177–183.
9. Савич-Шемет О.Г. Использование IEEE 802.1x в корпоративных сетях при внедрении тенденции BYOD // Современные средства связи. — 2020. — №1. — С. 233–235.
10. Корнеенков А.В., Коккоз М.М., Смагулова А.К. Повышение безопасности систем удаленного администрирования: защита информации // Universum: технические науки. — 2022. — №5–2(98). — С. 28–32.

Журнал «Современная наука: актуальные проблемы теории и практики»