УДК 004.9

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Владислав Александрович Шацкий
аспирант
shatskiy2000@list.ru
Владислав Олегович Чиркин
магистрант
abracadabr66@mail.ru
Наталья Викторовна Картечина
кандидат сельскохозяйственных наук, доцент
kartechnatali@mail.ru
Олег Викторович Тарасов
старший преподаватель
olegvtarasovyandex.ru@mail.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. Современные технологии обеспечения информационной безопасности в условиях нарастающих киберугроз.

Ключевые слова: информационная безопасность, киберугрозы, цифровые технологии.

В настоящее время цифровые технологии охватывают почти все аспекты нашей жизни, предоставляя удобство и комфорт, легкий доступ и эффективность в различных процессах и аспектах. Однако с этим также возрастает угроза появления новых типов и разновидностей киберпреступлений. Злоумышленники постоянно совершенствуют свои методы, делая их всё более сложными для обнаружения. Чтобы эффективно противостоять и сопротивляться вызовам, важно не только следить за новыми тенденциями в области кибербезопасности, но и активно применять передовые технологические решения.

Сегодня киберпреступники применяют разнообразные тактики для достижения своих целей. Фишинг (fishing «рыбная ловля, выуживание»), программы-вымогатели, манипуляции через социальную инженерию и атаки на устройства интернета вещей остаются наиболее распространёнными методами подверженными взлому. Кроме того, появились совсем новые виды угроз, такие как атаки на цепочки поставок (supplychainattacks), когда злоумышленники внедряют вредоносные программы через сторонние сервисы в программное обеспечение, используемое организациями.

Одной из наиболее серьёзных современных угроз являются атаки с применением искусственного интеллекта (ИИ). Хакеры используют ИИ для создания сложных и незаметных эксплойтов (Эксплóйт — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему), которые могут обходить стандартные системы защиты. Технологии ИИ позволяют сгенерировать правдоподобные фишинговые сообщения или письма, которые сложно отличить от настоящих.

В условиях постоянно меняющегося мира киберугроз, для компаний и частных лиц становится крайне важным заранее предпринимать меры предосторожности. Реакция на инциденты больше не является эффективной

стратегией: необходимо готовиться заранее к возможной атаке и иметь пошаговый план действий на случай её возникновения. Это подразумевает регулярное обновление программного обеспечения, применение многоуровневых систем защиты и осуществление регулярных проверок информационной безопасности.

Новые технологии играют важную роль в обеспечении защиты от киберугроз. Несколько основных направлений, которые в настоящее время наиболее актуальны.

Искусственный интеллект и машинное обучение продолжают оставаться важными инструментами для профессионалов в области кибербезопасности. Эти технологии способны обрабатывать большие объёмы данных, выявляя необычные активности и аномалии в реальном времени. Это позволяет быстро реагировать на угрозы, прежде чем они смогут вызвать значительный ущерб.

Например, ряд компаний разрабатывает системы, которые могут автоматически обучаться, используя поступающие данные, и адаптироваться к меняющимся условиям. Такие решения имеют возможность самостоятельно идентифицировать новые виды атак и предлагать действенные контрмеры.

Данная технология представляет собой абсолютно новый шаг в эволюции методов идентификации. Вместо традиционного применения паролей, поведенческая биометрия изучает уникальные черты поведения пользователя, такие как стиль печати, движения курсора, особенности голосовых команд и прочие параметры. Это делает авторизацию не только безопаснее, но и удобнее.

Поведенческая биометрия способствует снижению рисков мошенничества, так как даже если злоумышленник получит доступ, ему будет сложно воспроизвести поведение настоящего владельца учетной записи.

Модель “нулевого доверия” стала стандартом для крупных и средних организаций, желающих снизить риски. Основнаязадумка этой модели в том, что ни один из приборов или пользователей в корпоративной сети не

полностью доверен, и доступ предоставляется строго по мере необходимости, при этом каждый запрос на доступ с внимательно проверяется. Это усложняет злоумышленникам, проникнуть внутри сети, так как им приходится преодолевать множество уровней защиты, а не ставить всего один.

Важно понимать, что защита данных – это не одноразовая акция, а постоянный процесс. Компании должны регулярно пересматривать свои стратегии кибербезопасности, обновлять политики и процедуры, а также проводить тренинги для сотрудников. В условиях быстро развивающихся технологий и изменений в законодательстве, устаревшая система защиты может стать уязвимой.

Технологии продолжают развиваться, но человеческий фактор остается одним из самых слабых в системе защиты. К примеру, социальная инженерия активно используется преступниками для доступа к конфиденциальной информации. В связи с этим особое внимание следует уделить обучению работников основам кибербезопаности. Человек должен знать, как распознать фишинговое письмо и не перейти на ссылку, а также повидаться информацией о своих данных. Прохождение рабочих тренировок и симуляционных игр позволит сотрудникам лучше понять возможное воздействие угрозы и подготовиться к ним.

Более того, эффективная система кибербезопасности должна быть интегрирована с другими ИТ-системами компании. Это включает в себя взаимодействие с сетевыми устройствами, серверами, приложениями и базами данных. Интеграция такого рода позволяет своевременно обнаруживать и устранять уязвимости, а также обеспечивать согласованность политик безопасности на всех уровнях. Кроме того, многие современные платформы позволяют автоматические решать рутинные операции, включая обновление программного обеспечения и патчей, что сокращает время реагирования на новые угрозы.

Соблюдение требований, таких как General Data Protection Regulation в

Европе или «О персональных данных» в России, является обязательным условием для ведения бизнеса. Нарушение этих норм может привести к серьезным штрафам и репутационным потерям.

Организации должны на постоянной основе проверять соответствие своих процедур и систем требованиям законодательства, а также внедрять необходимые изменения для поддержания высокого уровня защиты данных от кибератак.

Благоприятные тенденции технологического прогресса и изменения законодательства заставляют менять стратегии работы в области кибербезопасности. Для фирм, желающих оставаться конкурентоспособными, это означает необходимо гибко и активно адаптироваться к новым вызовам. В случае системы тестирования и аудита обеспечения фирмы это также способствует повышению общей устойчивости компании к внешним угрозам.

Кибербезопасность – это сложный и многогранный процесс, требующий комплексного подхода. Использование передовых технологий, регулярное обучение персонала и соблюдение нормативных требований – ключевые элементы успешной стратегии защиты данных. Только совместными усилиями можно создать надежную систему, способную противостоять современным киберугрозам и обеспечить безопасность бизнеса в долгосрочной перспективе.

Список литературы:

1. Абалуев Р.Н., Кочетыгов А.И., Дорохова А.М., Шацкий В.А. Проектирование нейросетевой модели поведенческого анализа обучающегося электронной образовательной среды moodle // Наука и Образование. 2021. Т. 4. № 2.

2. Гущина А.А., Пчелинцева Н.В., Шацкий В.А. Применение искусственного интеллекта в обеспечении безопасности данных // В сборнике: Инженерное обеспечение инновационных технологий в АПК: Материалы

Международной научно-практической конференции. Мичуринск-наукоград РФ. 2021. С. 79-81.

3. Картечина Н.В., Дорохова А.М., Абалуев Р.Н., Шацкий В.А., Гущина А.А., Чиркин С.О. Виды нейронных сетей и их применение // Наука и Образование. 2021. Т. 4. № 3.

УДК 004.9

MODERN INFORMATION SECURITY TECHNOLOGIES

Vladislav Al. Shatskiy
postgraduate student
shatskiy2000@list.ru
Vladislav Ol. Chirkin
master's student
abracadabr66@mail.ru
Natalia V. Kartechina
phd, head of the department
kartechnatali@mail.ru
Oleg V. Tarasov
senior lecturer
olegvtarasovyandex.ru@mail.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. Modern technologies for ensuring information security in conditions of increasing cyber threats.

Keywords: information security, cyber threats, digital technologies.

Статья поступила в редакцию 11.11.2024; одобрена после рецензирования 20.12.2024; принята к публикации 25.12.2024.

The article was submitted 11.11.2024; approved after reviewing 20.12.2024; accepted for publication 25.12.2024.