КИБЕРБЕЗОПАСНОСТЬ ОПЕРАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Б. А. Ханчаев

Государственный энергетический институт Туркменистана, г. Мары

Глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств и мирового сообщества в целом. Информационные технологии применяются при решении задач обеспечения национальной, экономической безопасности и т. д. Основная роль заключается в защите конфиденциальных данных, доступ к которым может иметь только один авторизованный пользователь.

Ключевые слова: кибербезопасность, кибератака, защищенность, понятие, термин, определение, свойство, информация, безопасность.

Возрождение новой эпохи могущественного государства, налаживание работы цифровой системы по обеспечению кибербезопасности на современном уровне, дальнейшая модернизация этой деятельности согласно мировой практике весьма актуальны в контексте реализации «Концепции развития цифрово экономики в Туркменистане на 2019–2025 годы» и Государственной программы по развитию цифровой экономики в Туркменистане на 2021–2025 годы». Активное использование глобальной сети Интернет и других составных элементов киберпространства влечет за собой появление новых потенциальных вызовов [1].

Кибербезопасность можно описать как коллективные методы, технологии и процессы, помогающие защитить конфиденциальность, целостность и доступность компьютерных систем, сетей и данных от кибератак или несанкционированного доступа. Поскольку активы организации состоят из нескольких разрозненных систем, эффективная и действенная система кибербезопасности требует скоординированных усилий во всех ее информационных системах. Таким образом, кибербезопасность состоит из нижеперечисленных поддоменов.

Безопасность приложений включает реализацию различных средств защиты во всем программном обеспечении и службах, используемых в организации, от широкого спектра угроз. Это требует проектирования безопасных архитектур приложений, написания безопасного кода, реализации надежной проверки ввода данных, моделирования угроз и т. д., чтобы свести к минимуму вероятность любого несанкционированного доступа или модификации ресурсов приложения.

Сетевая безопасность включает в себя реализацию как аппаратных, так и программных механизмов для защиты сети и инфраструктуры от несанкционированного доступа, сбоев и неправильного использования. Эффективная сетевая безопасность помогает защитить активы организации от многочисленных внешних и внутренних угроз.

Мобильная безопасность относится к защите как организационной, так и личной информации, хранящейся на мобильных устройствах, таких как сотовые телефоны, ноутбуки, планшеты и т. д., от различных угроз: несанкционированного доступа, потери или кражи устройства, вредоносного программного обеспечения и т. д.

Облачная безопасность связана с разработкой безопасных облачных архитектур и приложений для организации с использованием различных поставщиков облачных услуг, таких как AWS, Google, Azure, Rackspace и т. д. Эффективная конфигурация архитектуры и среды обеспечивает защиту от различных угроз.

Формальное обучение сотрудников темам компьютерной безопасности имеет важное значение для повышения осведомленности о передовом опыте в отрасли,

организационных процедурах и политиках, а также для мониторинга и сообщения о злонамеренных действиях [2].

Учитывая быстро развивающийся технологический ландшафт и тот факт, что использование программного обеспечения постоянно растет в различных секторах, все больше и больше информации становится цифровой и доступной через беспроводную и проводную цифровую коммуникационную сеть и вездесущий Интернет. Высококонфиденциальная информация представляет большую ценность для злоумышленников, поэтому важно защищать ее с помощью надежных мер и процессов кибербезопасности.

Развивающийся технологический ландшафт также создает проблемы при реализации эффективных стратегий кибербезопасности. Программное обеспечение постоянно меняется, и, обновляясь, создает и ощущение уязвимости, так как подвержено различным кибератакам. Кроме того, ИТ-инфраструктура также развивается и многие компании уже переносят свои локальные системы в облако, что создает совершенно новые проблемы проектирования и реализации, следовательно, появляются дополнительные категории уязвимостей. Компании не знают о различных рисках в своей ИТ-инфраструктуре и не могут принять какие-либо контрмеры кибербезопасности, пока не станет слишком поздно.

Кибератака – это преднамеренная попытка внешних или внутренних угроз, или злоумышленников использовать и поставить под угрозу конфиденциальность, целостность и доступность информационных систем целевой организации или лица (лиц). Кибер-злоумышленники используют незаконные методы, инструменты и подходы для причинения ущерба и сбоев или получения несанкционированного доступа к компьютерам, устройствам, сетям, приложениям и базам данных.

Кибератаки бывают самыми разнообразными, и в приведенном ниже списке выделены некоторые из важных, которые злоумышленники используют для использования программного обеспечения [2]:

Вредоносное программное обеспечение

• Атаки путем внедрения (например, межсайтовый скриптинг, внедрение SQL, внедрение команд).

• Управление сессиями и атаки «человек посередине».

Фишинг

• Отказ в обслуживании.

• Повышение привилегий.

• Неисправленное/уязвимое программное обеспечение.

• Удаленное выполнение кода.

• Грубая сила.

Лучшая практика управления кибербезопасности

Проведите обучение и повышение осведомленности о кибербезопасности. Сильная стратегия кибербезопасности не будет успешной, если сотрудники не будут обучены темам кибербезопасности, политике компании и отчетности о происшествиях. Даже самая лучшая техническая защита может выйти из строя, когда сотрудники совершают непреднамеренные или преднамеренные злонамеренные действия, что приводит к дорогостоящему нарушению безопасности. Обучение сотрудников и повышение осведомленности о политиках компании и передовых методах обеспечения безопасности с помощью семинаров, занятий и онлайн-курсов – лучший способ уменьшить небрежность и вероятность нарушения безопасности.

Обеспечьте управление уязвимостями и управление исправлениями/обновлениями программного обеспечения. Для ИТ-отделов организации крайне важно вы-

полнять идентификацию, классификацию, исправление и устранение уязвимостей во всем программном обеспечении и сетях, которые они используют, чтобы уменьшить угрозы для своих ИТ-систем. Кроме того, исследователи безопасности и злоумышленники время от времени выявляют новые уязвимости в различном программном обеспечении, о чем сообщают поставщикам программного обеспечения или публикуют их. Эти уязвимости часто используются вредоносными программами и кибератаками. Поставщики программного обеспечения периодически выпускают обновления, которые исправляют и устраняют эти уязвимости. Таким образом, поддержание ИТ-систем в актуальном состоянии помогает защитить активы организации.

Обеспечьте безопасное хранение паролей и политики. Организации должны обеспечить использование надежных паролей, соответствующих рекомендуемым отраслевым стандартам, для всех сотрудников. Их также следует принудительно периодически менять для защиты от скомпрометированных паролей. Кроме того, хранилище паролей должно соответствовать лучшим отраслевым практикам использования солей и надежных алгоритмов хеширования.

Проводите периодические проверки безопасности. Периодическая проверка безопасности всего программного обеспечения и сетей помогает выявить проблемы безопасности на ранней стадии и в безопасной среде. Проверки безопасности включают в себя тестирование на проникновение приложений и сетей, проверку исходного кода, проверку архитектуры, оценку красной команды и т. д. После обнаружения уязвимостей в системе безопасности организации должны расставить приоритеты и устранить их как можно скорее.

Резервное копирование данных. Периодическое резервное копирование всех данных повысит избыточность и гарантирует, что все конфиденциальные данные не будут потеряны или объединены после нарушения безопасности. Такие атаки, как инъекции и программы-вымогатели ставят под угрозу целостность и доступность данных. Резервные копии могут помочь защитить в таких случаях.

Используйте шифрование для данных в состоянии покоя и в пути. Вся конфиденциальная информация должна храниться и передаваться с использованием надежных алгоритмов шифрования. Шифрование данных обеспечивает конфиденциальность. Следует также внедрить эффективное управление ключами и политику ротации. Все веб-приложения/программное обеспечение должны использовать SSL/TLS.

Разрабатывайте программное обеспечение и сети с учетом безопасности. При создании приложений, написании программного обеспечения, проектировании сетей всегда проектируйте их с учетом безопасности. Имейте в виду, что затраты на рефакторинг программного обеспечения и последующее добавление мер безопасности намного выше, чем создание системы безопасности с самого начала. Приложение, разработанное для обеспечения безопасности, помогает уменьшить угрозы и гарантирует, что в случае сбоя программного обеспечения сетей они будут безопасными [5].

Литература

1. Концепция развития цифровой экономики в Туркменистане на 2019–2025 годы. – Ашхабад, 2018.
2. The Cyber Security Body of Knowledge. The National Cyber Security Centre: 2019.
3. Петренко, С. Киберустойчивость цифровой экономики. Как обеспечить безопасность и непрерывность бизнеса / С. Петренко. – СПб. : Питер, 2021. – 384 с.