УДК 004.056(075.8)

О. Е. Корнеенко
okorneenko@gsu.by
ГГУ имени Ф. Скорины, Республика Беларусь

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВАЖНОСТЬ ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ПУТИ РЕШЕНИЯ

Данная статья посвящена актуальным на сегодняшний день проблемам информационной безопасности в информационных системах. Особое внимание уделено автоматизированным системам обработки учетно-аналитической информации бухгалтерии организаций. Также в статье рассмотрены эффективные решения для преодоления изложенных проблем.

Ключевые слова: информационная безопасность, автоматизированная система, проблема, программное обеспечение, социальная инженерия, защита данных, несанкционированный доступ, аутентификация.

Информационная безопасность является одной из самых важных тем в современном цифровом мире. В наше время, когда цифровые технологии проникают во все сферы нашей жизни, эта проблема становится особенно актуальной. Электронные данные и информационные системы изменяют любые угрозы, такие как хакерские атаки, вирусы и утечка данных. С появлением кибератак и утечек информации сохранение безопасности становится приоритетной задачей для организаций, правительств и мировых деятелей [1]. В данной статье мы рассмотрим некоторые основные проблемы информационной безопасности, включая автоматизированные системы обработки данных в бухгалтериях организаций, и предложим эффективные решения для их решения.

Первая проблема, на которой стоит сосредоточить внимание, это использование устаревших систем и уязвимого программного обеспечения. Это одна из основных причин, почему информационная безопасность превращается в опасность. Устаревшие системы и программы часто оказываются слабыми, и мировые злоумышленники могут воспользоваться для проведения кибератак. Ошибка в коде может привести к несанкционированному доступу к системе. Решение этой проблемы заключается в периодическом обновлении системы и программного обеспечения, а также внедрении уязвимостей в Диптихах и своевременном их исправлении. Патчи, созданные разработчиками, также следует хранить, проводя аудит безопасности приложений, чтобы выявить потенциальные уязвимости.

Вторая проблема, с которой возникли проблемы у организаций, – это социальная инженерия. Это метод манипуляции людьми для доступа к конфиденциальной информации. Злоумышленники могут использовать различные методы, такие как фишинг, для получения логинов, паролей и других учетных данных. Чтобы справиться с этой проблемой, необходимо проводить регулярные тренинги по безопасности и повышать компетентность сотрудников в отношении таких атак. Внедрение многофакторной аутентификации и использование надежных паролей также могут снизить риск социальной инженерии.

Третья проблема, на которую стоит обратить внимание, – это недостаточная защита медицинских данных. Утечка, опасность или потеря данных становятся все более серьезной проблемой для информационной безопасности. С учетом объема цифровых данных, их сбора и хранения защита этих данных становится все более важной. Частные утечки данных и хакерские меры подрывают конфиденциальность и конфиденциальность личной информации. Для решения этой проблемы следует использовать методы защиты, усилить меры безопасности и соблюдать соответствующие законодательные нормы.

Следующая проблема – это недостаточная осведомленность о мерах защиты информации. Большое количество пользователей и организаций не имеют достаточного понимания о методах обеспечения безопасности информации. Разрешение этой проблемы может предусматривать обучение пользователей принципам информационной безопасности и распространение сведений о значимости сохранности данных среди организаций.

Ещё одной из основных проблем является увеличение сложности методов нападения. С течением времени и развитием технологий, методы, используемые злоумышленниками, становятся все более сложными. Это может включать использование искусственного интеллекта, распределение атак на разные части сети и эксплойты нулевых дней. Для эффективной борьбы с этими угрозами, важно проводить постоянное обновление и апгрейд системы безопасности, регулярное обучение персонала и реализацию защитных мер, таких как файрволы, системы обнаружения вторжений и антивирусное программное обеспечение.

Итак, вопросы информационной безопасности представляют серьезную угрозу для организаций и отдельных пользователей. Разрешение этих вопросов требует интегрированного подхода, который включает в себя обновление систем и программного обеспечения, обучение пользователей, защиту личных данных и распространение информации о средствах безопасности. Только объединяя наши усилия, мы сможем эффективно справиться с проблемами информационной безопасности и создать защищенное цифровое пространство для всех.

Автоматизированные системы бухгалтерии для обработки учетно-аналитической информации становятся все более популярными в современном мире бизнеса. Они облегчают и ускоряют процессы учета и отчетности, что повышает производительность организаций и предприятий. Но наряду с преимуществами, автоматизированные системы бухгалтерии также несут в себе определенные риски для информационной безопасности [2]. Давайте рассмотрим важность обеспечения информационной безопасности в автоматизированных системах для обработки учетно-аналитической информации и предложим некоторые решения для минимизации этих рисков.

1. Защита секретной информации. Автоматизированные системы бухгалтерии хранят в себе большое количество секретной информации, включая финансовые данные, персональную информацию сотрудников и клиентов. Поэтому одной из критически важных задач в современном мире информационных технологий является защита секретной информации в таких системах. Этого можно достигнуть путем регулярного обновления систем и программного обеспечения, установки фаерволов и антивирусного программного обеспечения, а также применения шифрования для хранения и передачи данных. Важным также является ограничение доступа к системе только для авторизованных сотрудников и проведение регулярного обучения по вопросам безопасности с ними.

Вот несколько ключевых мер, которые можно принять для обеспечения сохранности секретных данных в автоматизированных системах:

– установление и поддержание надежных систем безопасности: безопасность автоматизированных систем начинается с установки и поддержания эффективных систем безопасности, включая файрволы, антивирусное программное обеспечение и системы обнаружения вторжений. Эти системы защищают информацию от несанкционированного доступа и вредоносного программного обеспечения;

– использование аутентификации и авторизации: аутентификация и авторизация являются важными мерами безопасности. В автоматизированных системах должны быть реализованы солидные механизмы аутентификации для проверки личности пользователей и системы авторизации для определения уровня доступа. Механизмы аутентификации используются для проверки подлинности пользователя и предоставления доступа к системе или ресурсам. Вот несколько распространенных механизмов аутентификации:

а) что-знает пользователь (Something You Know): этот метод основан на знании уникальной информации, такой как пароль, PIN-код или ответ на секретный вопрос;

б) что-имеет пользователь (Something You Have): этот метод включает использование физического объекта в качестве идентификатора, такого как магнитная карта, ключ или аутентификатор (токен) с одноразовыми паролями;

в) что-такое пользователь (Something You Are): этот метод использует биометрические данные, такие как скан отпечатка пальца, распознавание лица, голоса или сетчатки глаза, чтобы идентифицировать пользователя;

г) что-то, что уникально для пользователя (Something Unique to You): этот метод предполагает использование уникальных параметров, таких как отпечаток пальца, голографический образ или электрический импульс, которые уникальны для конкретного пользователя;

д) что-то, что пользователь делает (Something You Do): этот метод включает использование поведенческих характеристик, таких как способ печати на клавиатуре, образец движения мыши или фразы, чтобы идентифицировать пользователя.

Часто используются комбинации этих методов, и такой подход называется многофакторной аутентификацией (MFA). Например, использование пароля в сочетании с одноразовым кодом, получаемым на мобильный телефон пользователя. Это повышает надежность и безопасность процесса аутентификации:

– шифрование данных: применяя методы шифрования для хранения и передачи данных, можно обеспечить сохранность секретной информации, даже если произойдет утечка информации;

– проведения регулярных обновлений и исправлений: необходимо регулярно обновлять программные компоненты и операционные системы, чтобы исправить известные уязвимости и вопросы безопасности. Установка исправлений и обновлений помогает предотвратить несанкционированный доступ и взлом системы;

– обучение персонала: политика конфиденциальности также зависит от обучения персонала. Регулярные тренинги по безопасности помогают повысить осведомленность сотрудников о мерах защиты и предотвращения угроз безопасности;

– резервное копирование и восстановление: регулярное резервное копирование данных и наличие плана восстановления после катастрофы обеспечат быстрое восстановление данных после инцидента, препятствует потере данных и способствует быстрому восстановлению операций.

2. Препятствие процессу неавторизованного доступа. Неразрешенный вход в автоматизированные бухгалтерские системы может вызвать искажение данных, незаконное присвоение финансовых средств или утечку конфиденциальной информации. Блокировка неразрешенного входа в бухгалтерские автоматизированные системы является ключевым для охраны финансовой информации организации. Для предотвращения подобных ситуаций требуется применение многофакторной аутентификации, сложных паролей и безопасностных протоколов. Регулярно необходимо исправлять и обновлять политики доступа, а также проводить мониторинг действий пользователей, чтобы незамедлительно обнаружить любые сомнительные действия. Дадим несколько рекомендаций по этому направлению минимизации рисков использования автоматизированных систем бухгалтерии:

– важно использовать сложные пароли из комбинации букв, цифр и символов, которые должны быть уникальными для каждой учетной записи и регулярно обновляться;

– рекомендуется включить аутентификацию в двух факторах (2FA), которая позволяет ввести дополнительный проверочный код после ввода пароля. Это усложняет процесс неавторизованного доступа, даже если кто-то получил доступ к определенному паролю;

– необходимо установить строгие права доступа для ограничения доступа к бухгалтерским системам только уполномоченным сотрудникам. Каждый пользователь должен иметь только необходимые права для выполнения своих задач в рамках конкретного функционала;

– постоянный мониторинг активности пользователей в бухгалтерской системе позволяет обнаружить любые подозрительные действия или необычную активность, которая может указывать на неавторизованного доступ или взлом;

– использование шифрования данных для защиты конфиденциальной информации в бухгалтерской системе позволяет защитить эти данные в случае неавторизованного доступа или утечки информации;

– регулярное создание резервных копий данных является важным шагом для защиты от потери данных в случае неавторизованного доступа или технического сбоя.

3. Увеличение сложности атак. С процессом технологического развития, злоумышленники постепенно усложняют свои методы атак. Это включает применение искусственного интеллекта, последовательное нападение на различные уровни сети и названные «zero-day» угрозы. Для эффективного сопротивления этим угрозам, необходимо проводить постоянное обновление и модернизацию системы безопасности, регулярное обучение персонала, и применение защитных мер, таких как файрволы, системы обнаружения вторжений, и антивирусное программное обеспечение.

Таким образом, автоматизированные системы бухгалтерии, которые обрабатывают учетно-аналитическую информацию, становятся все более широко используемыми в современном деловом мире. Они помогают значительно упростить и ускорить процессы учета и отчетности, что повышает эффективность работы организаций и предприятий. Однако, вместе с преимуществами, автоматизированные системы бухгалтерии также представляют определенные риски для информационной безопасности.

Проблемы информационной безопасности представляют значительную угрозу для организаций и индивидуальных пользователей. Решение этих проблем требует комплексного подхода, который включает в себя обновление систем и программного обеспечения, обучение пользователей, защиту личных данных и распространение информации о средствах обеспечения безопасности. Только через объединенные усилия мы сможем эффективно справиться с проблемами информационной безопасности и создать безопасное цифровое пространство для каждого.

Литература

1. Латыпова, Э.Р. Проблемы защиты информации / Э.Р. Латыпова. – М.: Уфа. – 2017.

2. Бормотов, В. Е. Проблемы защиты информации в компьютерной сети / В.Е. Бормотов. – М.: Молодой ученый, №11(115). – 2016.