Аппаратура фидерной защиты и автоматики (АФЗА) является модернизированной версией аппаратуры защиты (АЗМ2). Аппаратура фидерной защиты и автоматики (АФЗА) предназначена для эксплуатации в составе комплектного распределительного устройства совместно с быстродействующим выключателем (БВ) на тяговых подстанциях городского транспорта постоянного тока напряжением до 1,0 кВ (0,825 кВ для метрополитена и 0,630 кВ для трамвая, троллейбуса).

АФЗА используется в качестве основной защиты фидера, дополнительно к используемой защите БВ, осуществляемой реле дифференциальным шинным (РДШ).

Система мониторинга и защиты тяговой сети серии SMTN-3 предназначена для применения в качестве устройства защиты тяговой сети от токов короткого замыкания и недопустимых перегрузок, мониторинга параметров тяговой сети, применения в качестве устройства накопления данных для последующего анализа произошедших аварийных процессов.

SMTN-3 используются в распределительных устройствах (РУ) тяговых подстанций городского транспорта, метрополитена, электрифицированных железных дорог, промышленных предприятий, а также для предприятий горнодобывающей промышленности. Устройство не включает в себя функцию АУВ, поэтому подразумевается использование совместно с уже существующей схемой управления и АПВ выключателя или с отдельным терминалом АУВ. Устройство является комбинированным микропроцессорным устройством релейной защиты. Применение в устройстве модульной микропроцессорной архитектуры наряду с современными технологиями поверхностного монтажа обеспечивают высокую надежность, большую вычислительную мощность и быстродействие, а также высокую точность измерения электрических величин и временных интервалов, что дает возможность повысить чувствительность защитных функций. Реализованные в устройстве алгоритмы функций защиты и автоматики, а также схемы подключения устройства разработаны в сотрудничестве с представителями энергосистем, что облегчает внедрение новой техники проектировщикам и эксплуатационному персоналу. Элементная база входных и выходных цепей обеспечивает совместимость SMTN-3 с любыми типами устройств автоматики разных производителей – электромеханическими, электронными, аналого-цифровыми, микропроцессорными.

**Список литературы**

1 **Шнеерсон, Э. М.** Цифровая релейная защита / Э. М. Шнеерсон. – М. : Энергия, 2007. – 198 с.

2 **Быков, Е. И.** Электроснабжение метрополитенов. Устройство, эксплуатация и проектирование / Е. И. Быков. – М. : Транспорт, 1977. – 431 с.

УДК 004.416.6

## ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМЫ 1С: БУХГАЛТЕРИЯ ДЛЯ БЮДЖЕТНЫХ УЧРЕЖДЕНИЙ

*Т. С. ГРОМЫКО, Д. В. ВЕРБЕНЕЦ*
*Белорусский государственный университет транспорта, г. Гомель*

На территории СНГ самым распространенным продуктом для автоматизации хозяйственной деятельности в организациях является 1С: Предприятие. Беларусь не стала исключением: многие предприятия и организации, как частные, так и государственные, ведут учёт с помощью системы 1С или осуществляют плавный переход на данный программный продукт.

База данных 1С является огромным источником информации, в неё постоянно вносят дополнения, изменяют, просматривают. К этой базе данных, зачастую, имеет доступ огромное количество людей, например, бухгалтер, программист, руководитель организации или проверяющее лицо. Чем больше людей с различными служебными и должностными обязанностями имеют доступ к системе, тем больше существует возможных угроз для утечки, модификации или повреждения информации.

Концепция информационной безопасности основывается на трех основных факторах: целостность, конфиденциальность и доступность информации. Целостность – гарантия сохранности данными верных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные. Доступность – гарантия того, что авторизованные пользователи всегда получат доступ к данным. Конфиденциальность – гарантия того, что определенные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).

В любой сфере, которая ведёт электронный учёт, особенно важны факторы информационной безопасности. Контроль над соблюдением каждого из этих условий следует осуществлять таким образом, чтобы не нарушить работы всей системы в целом. Для этого требуется надлежащим образом поддерживать доступность системы, при этом не нарушая конфиденциальность и целостность информации базы данных.

Процесс развития систем 1С: Предприятие продолжается на протяжении 20 лет. За это время платформа 1С претерпела множество изменений и несколько глобальных перерождений. Последней актуальной версией является 1С: Предприятие 8.

На примере Белорусского государственного университета транспорта (далее – БелГУТ): был осуществлен переход с программного продукта 1С: Бухгалтерия 7.7 на актуальную версию.

С выходом современных систем 1С требования к защите информации постоянно возрастают. Версия 7.7 давно утратила свою актуальность. Реализуемая концепция безопасности в данной версии не удовлетворяет современным требованиям развития информационных систем: низкая масштабируемость, высокая степень доступности данных и недостаточная защищенность системы. Из-за большого отличия в принципах и методах ее работы (построения и функционирования) от версии 8, более детально рассматривать её в данной статье будет нецелесообразно.

Что касается версии 8, то существует два основных способа реализации работы системы 1С [1]:

– файловый вариант;

– клиент-серверный вариант.

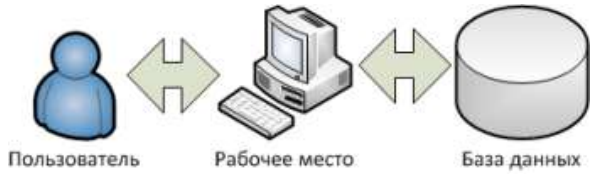


Рисунок 1 – Файловый вариант

Файловый вариант подразумевает под собой одновременное хранение базы данных и работу пользователя на одном персональном компьютере (рисунок 1). Конфигурация и база данных хранятся на одном локальном диске, который доступен любому пользователю операционной системы. Это ключевое отличие дает неограниченные возможности по обходу системы защиты 1С.


Рисунок 2 – Клиент-серверный вариант

От данного недостатка избавлены организации, которые избрали клиент-серверный вариант работы (данный вариант реализован в БелГУТе), который подразумевает под собой контакт пользователя с базой данных через сервер 1С, что, в свою очередь, значительно снижает возможности злоумышленника (рисунок 2). Данный вариант подразумевает под собой цепочку звеньев, каждое из которых участвует в процессе взаимодействия пользователя с базой данных [2]. На каждом из этих этапов существуют определенные уязвимости, связанные с пересылкой информации, хищением или повреждением данных. Приведём основные угрозы для системы 1С: Бухгалтерия:

– простые пароли пользователей системы;

– хранение паролей на листках бумаги, в памяти компьютера;

– использование старых логинов;

– вирусы;

– шпионские программы;

– перехват информации;

– открытый доступ пользователей к административным функциям;

– уязвимости операционной системы;

– уязвимости системы управления базами данных (далее – СУБД);

– отсутствие разграничений прав доступа в 1С;

– возможность доступа к данным сервера СУБД.

Многие уязвимости следует закрыть (или уменьшить риск их использования) еще на этапе внедрения и первоначальной настройки системы 1С. Базовая (коробочная) версия программы имеет минимальный набор ролей, пользователей и интерфейсов, которые могут использоваться лишь в качестве шаблонов для последующей настройки системы доступа.

Права и роли относятся к предметной области решений на основе 1С: Предприятие 8 – такой подход позволяет разрабатывать «коробочные» решения, не ориентируясь на внедрение в конкретную организацию или предприятие. Права определяют доступ к отдельным объектам конфигурации, роли определяют доступ к решению в целом, это позволяет управлять разграничением доступа на уровне администрирования системы. Стандартное (коробочное) решение является черновым, потому следует создать свои собственные роли, исходя из специфики работы организации. Тот же принцип касается интерфейсов и пользователей системы 1С: Бухгалтерия.

Защита от несанкционированного использования системы 1С: Предприятие может быть реализована с помощью следующих механизмов [3]:

– сетевого лицензионного ключа HASP4 Net;

– программного лицензирования.

Данные механизмы обеспечивают одновременную работу пользователей с системой 1С: Предприятие. При этом пользователи могут находиться как в рамках локальной сети, так и за ее пределами, например, при использовании веб-клиентов (доступ через браузер) или тонких клиентов, подключенных через веб-сервер.

Фирма 1С рекомендует следующие советы по настройке безопасности системы 1С:

– ограничить физический доступ к серверам;

– обеспечить бесперебойную работу серверов;

– установить и своевременно обновлять брандмауэры на серверах;

– присваивать пользователям сложные пароли;

– производить смену паролей через определенный промежуток времени;

– предоставлять пользователям достаточный набор прав, необходимый для их комфортной работы, исключая права, которые отвечают за административные действия;

– следить, чтобы на всех компьютерах с установленной системой 1С были установлены, включены и своевременно обновлялись антивирусные системы;

– ограничить и регламентировать доступ к сети Интернет;

– настроить системный аудит событий безопасности;

– допускать к работе с системой только квалифицированных пользователей;

– закрыть и опломбировать все системные блоки;

– не допускать к персональным компьютерам посторонних лиц;

– своевременно выгружать базу данных, создавать резервные копии;

– установить на рабочие места актуальную версию Windows.

В БелГУТе на этапе внедрения 1С: Бухгалтерия 8 были реализованы рекомендации, которые касаются ролевого разграничения доступа, администрирования системы, а также работы серверов 1С и SQL. Прочие меры можно внедрить в процессе поддержки данного программного продукта.

Перечисленный выше комплекс мероприятий не является исчерпывающим и гарантирующим полную защиту системы 1С: Предприятие. Тем не менее, эти действия важно реализовать на этапе внедрения системы, так как это значительно снизит риски с учётом существующих уязвимостей. Далее, на этапе поддержки и сопровождения системы, следует продолжить контроль за соблюдением перечисленных мер. Администратору системы также следует своевременно реализовывать актуальные обновления платформы и конфигурации 1С, а также отслеживать новые уязвимости системы.

**Список литературы**

1 Профессиональная разработка в системе 1С: Предприятие 8 / под ред. М. Г. Редченко. – М. : 1С-Паблишинг. – Спб. : Питер, 2006. – 808 с.

2 1С: Предприятие. Клиент-серверный вариант. Руководство администратора / А. Алексеев [и др.]. – 2-е изд. – М. : Фирма «1С», 2011. – 170 с.

3 1С: Предприятие. Руководство администратора / А. Алексеев [и др.]. – 2-е изд. – М. : Фирма «1С», 2011. – 297 с.