UDC 657.1.

Кривошеева А.Е.
Методист вводных уроков
онлайн школа английского языка SkyEng, г. Киев Украина

МОДЕЛИ И МЕТОДЫ АНАЛИЗА ПРИМЕНЕНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ БУХГАЛТЕРСКОГО УЧЕТА

Аннотация. *Обеспечение стабильного и максимально эффективного функционирования и развития любого предприятия является основной задачей безопасности экономической информации. Ценнейшей экономической информации является учетная информация, которая характеризует все аспекты хозяйственной деятельности. Сегодня большинство субъектов хозяйствования используют компьютеризированную форму ведения бухгалтерского учета, которая предполагает использование специализированного программного обеспечения и технических средств.*
Ключевые слова: *учет, безопасность, анализ систем, методы, модели.*

В течение последних лет все более широкое использование перспективных ИТ-технологий обусловило не только многочисленные преимущества, но и целый ряд проблем. В частности, существенно повысился уровень информационного негативного влияния на процессы сохранения и распространения информации, возросла численность новых угроз информационной безопасности, таких как новые формы кибератак.

Термин "защита" означает способ обеспечения безопасности в системе обработки данных (SOD). Однако решение этой задачи значительно усложняется при организации компьютерной обработки бухгалтерской информации в среде коллективного использования, где концентрируются, перерабатываются и накапливаются сведения о различные цели и аксессуары. В системах

коллективного использования бухгалтерской информации с хорошо развитой сетью терминалов основной сложностью обеспечения безопасности является то, что потенциальный вторжения является полным абонентом системы. Вот основные объективные причины, которые определяют необходимость обеспечения информационной безопасности [3]:

– повышение скорости количественного и качественного роста использования компьютеров и увеличение их использования;

– постоянное увеличение количества новых видов и объемов информации, которую человек должен воспринимать и обрабатывать во время его деятельности;

– необходимость более эффективного использования ресурсов в экономике предприятия путем научного прогресса, направленной на принятие обоснованных решений на разных уровнях управления;

– высокая степень концентрации информации в центрах ее обработки.

Защита бухгалтерской информации обычно ограничивается выбором контроля за выполнением программ, имеющих доступ к информации, хранящейся в ОРВ. Поэтому создание систем записи информации требует сосредоточения внимания на защите пользователей учетных данных друг от друга, а также от случайной и целевой угрозы нарушением целостности данных [3]. Кроме того, механизмы, принятые для обеспечения безопасности бухгалтерской информации, должны предоставить пользователю средства для защиты своих программ и данных от себя.

Увеличение количества абонентов, которые используют услуги ИТ-системы, взаимодействии разных компьютеров в обмене информацией с подключенными к ним удаленными подключенными устройствами, создают сложные информационные и компьютерные сети [5]. Поэтому становится невозможным установление несанкционированного доступа к информации. Усложнение процесса вычисления на компьютере, что работает в багатопрограмному и многопроцессорном режиме, создает условия для

поддержания связи со значительным количеством абонентов. Это становится важным для решения проблемы физической защиты информации и сохранения информации от других пользователей или несанкционированного подключения пользователя, специально закрепленный в процессе расчета.

Поэтому необходимо установить требования к системе для обеспечения безопасности бухгалтерской информации, включая такие пункты, как [4]:

– отдельная идентификация отдельных пользователей и терминалов;
– создание отдельных программ (задач) за названием и функцией;
– контроль данных бухгалтерского учета, если необходимо, до уровня записи или элемента.

Ограничить доступ к информации для подключения следующих методов [5]:

– классификация иерархического доступа;
– классификация бухгалтерской информации по значимости и месту ее возникновения;
– указания на конкретные ограничения и их применение в информационных объектах, например, пользователь может прочитать файл без права записи.

Система защиты информации должна обеспечивать идентификацию, авторизацию, выявления и документацию всех видов учетных данных. Количество организационных требований системы защиты информации включает:

– ограничение доступа к компьютерной системе (регистрация и обслуживание посетителей);
– контроль изменений в программной системе;
– тестирование и проверка изменений в программной системе и программах защиты;
– поддерживать взаимный контроль за выполнением принципов защиты данных;

– установление ограничений на льготы персонала, обслуживающего СОД, которые соответствуют гарантийным требованиям в случае нарушения;

– создание записей о доступе к системе, а также к компетенции службы. Поэтому целесообразно разрабатывать и утверждать письменные инструкции [5]:

– начало и прекращение работы бухгалтерской информационной системы;

– контролировать использование магнитных лент, дисков, карт, списков,

– отслеживать порядок изменения программного обеспечения и внести эти изменения до пользователя;

– о процедуре восстановления системы в случае чрезвычайной ситуации.

– относительно правил ограничения разрешенных визитов до компьютерного центра;

– определить сумму предоставленной бухгалтерской информации.

В то же время важно разрабатывать систему для регистрации использования компьютеров для ввода данных и результатов, обеспечения периодической очистки ленточных архивов и журналов, дисков, карт для устранения и устранения неиспользованных; бухгалтерские документы согласно установленных стандартов [2].

Важно помнить, что все типы защиты взаимосвязаны, и если один из них не выполняет свои функции, усилия других сводится к нулю. Преимущества защиты программного обеспечения можно объяснить низкими издержками и легкостью разработки.

В последнее время так называемые электронные ключи стали обычным явлением. Это устройство подключается к компьютеру через порт LPT [4]. В этом случае электронный ключ не мешает нормальному функционированию

параллельного порта и полностью "прозрачен" для принтера и других устройств. Ключи могут быть каскадными и цепными, а разные типы ключей могут управлять разными компаниями.

Кроме того, они могут выполнять различные функции, такие как защита программ от несанкционированного копирования, а также может выявить тот факт, что защищенная программа была инфицирована различными типами файловых вирусов. При использовании электронных клавиш для генерации ключей шифрования не нужно помнить или хранить их, а затем вводить их с клавиатуры. Ключ не имеет встроенных источников питания и сохраняет информацию, хранящуюся в ней, после отключения от компьютера. Наиболее распространенными ключами в настоящее время есть ключи американской компании "Software Security Inc". Эта компания производит ключи для систем DOS, WINDOWS, UNIX, OS / 2 и Macintosh.

Электронные ключи могут быть одноразовыми или перепрограммированными, и могут содержать энергонезависимую память.

Кроме того, обычные пластиковые идентификационные карты (ИК) с достаточно большой емкостью памяти, что позволяет ограничить несанкционированный доступ к бухгалтерской информации. Это оборудование - программный комплекс состоит из следующих частей: специальной карты, которая вставляется в гнездо для расширения ПК, читателя ИК-информации и самой ИК; Часть программного обеспечения: драйверы для управления пластиной и инфракрасным считывателем.

Часть программного обеспечения комплекса может также включать в себя программное обеспечение для организации контроля доступа к части и раздела жесткого диска, с помощью запроса пароля. Поэтому вход в систему на украденной карточке исключен. Примером такого оборудования - комплексом программного защиты - может быть разработка Datamedia. Компьютерная серия Netmate оснащена специальным устройством для чтения карт памяти Securecard.

Стоит осознать, что проблема кибербезопасности – это проблема не только общегосударственного уровня, а каждого отдельно взятого предприятия. Понятно, что невозможно достичь стопроцентной безопасности для защиты учетных данных. Однако индивидуальная ответственность каждого работника бухгалтерской службы является самым первым и самым простым фактором, который способствует защите ценной учетной информации. Таким образом, на каждом предприятии должна быть создана программа определенных действий, направленных на создание кибернетической защиты учетной информации, сфера применения которого распространяется на человеческие ресурсы и не ограничивается исключительно технологическими аспектами. Перспективой дальнейших исследований может быть анализ угроз и современных средств поддержки кібезбезпеки учетной информации.

Список источников:

1. Васковская Н.С. Информационные системы учета: Учеб. пособие для студентов специальности „Учет и аудит”. – Хмельницкий: ТУП, 2013
2. Завгородний В.П. Автоматизация бухгалтерского учета, контроля, анализа и аудита. – К.: А.С.К., 2008
4. Ильина А.П. Информационные технологии бухгалтерского учета. – СПб.: Питер, 2011
5. Івахненков С.В. Информационные технологии в организации бухгалтерского учета и аудита: Учеб. пособие. – К.: Знание, 2014
6. Информационные системы в бухгалтерском учете / под ред. проф. Ф.Ф. Бутынца. – Житомир: ПП “Рута”, 2012