УДК 33

# *ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ УЧЕТНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ*

***Грицук Н.В.***

*к.э.н., доцент,*

*Вятский Государственный Университет,*

*Киров, Россия*

***Зянчурина К. Е.***

*студент,*

*Вятский Государственный Университет,*

*Киров, Россия*

**Аннотация:** Обеспечение защищенности любого вида является приоритетным направлением для каждого хозяйствующего субъекта. Для полноценной и эффективной работы предприятия необходимо гарантировать целостность, структурированность и защищенность учетной информации, однако, в настоящее время существует обширное множество информационных рисков и угроз, которые могут подорвать стабильность компании. С течением времени и развитием нанотехнологий, количество угроз неуклонно растет, именно это стало поводом для обозначения проблемы и проведения нами исследования. В результате проведенного анализа были выделены методы, которые помогут предотвратить и предупредить процесс хищения, искажения или уничтожения конфиденциальной информации третьими лицами.

Целью данного исследования является выявление основных угроз для безопасности учетной информации организации и выявление путей ее максимальной защиты. Предмет исследования – информационная безопасность организации. В статье рассмотрены основные угрозы для безопасности учетной информации, которые могут негативно повлиять на работу хозяйствующего субъекта и современные способы защиты конфиденциальных данных.

**Ключевые слова:** информационная безопасность организации, учетная информация, внутренний контроль, информационные риски, экономическая безопасность.

## *ENSURING THE ECONOMIC SECURITY OF ACCOUNTING INFORMATION AT THE ENTERPRISE*

***Gritsuk N.V.***
*PhD, Associate Professor,*
*Vyatka State University,*
*Kirov, Russia*
***Zyanchurina K.E.***
*student,*
*Vyatka State University,*
*Kirov, Russia*

**Abstract:** Ensuring the protection of any kind is a priority for each business entity. For the full and effective operation of the enterprise, it is necessary to guarantee the integrity, structurization and security of accounting information however, at present there is an extensive set of information risks and threats that may undermine the stability of the company. Over time and the development of nanotechnologies, the number of threats is growing steadily; this is the reason is for the problem and our research. As a result of the analysis, methods were identified that would help prevent and prevent the process of theft, distortion or destruction of confidential information by third parties.

The purpose of this study is to identify the main threats for the security of the organization's accounting information and identify the ways of its maximum protection. The subject of the study is the information security of the organization. The article discusses the main threats to the security of accounting information, which can negatively affect the work of an economic entity and modern methods of protecting confidential data.

**Keywords:** information security of the organization, accounting information, internal control, information risks, economic security

Любое предприятие, будь то малое, среднее или крупное, является открытой системой, на которое оказывают влияние как экзогенные факторы, например, открытия науки, техники, политические события, так и эндогенные, присущие любой экономической системе – ситуации с ценными бумагами, инвестициями, работа с персоналом и самим процессом производства организации.

Для обеспечения стабильного роста предприятия и, как следствие, эффективного ведения бухгалтерской отчетности организации необходимо гарантировать информационную безопасность данных. В эпоху расцвета современных технологий происходит развитие киберпреступности, повышение уровня недобросовестной конкуренции, коррупции и расширение влияния нелегального сектора. Из-за этого очень важно обеспечить оперативное предотвращение утечек конфиденциальной информации. В последнее время во всем мире наблюдается рост достаточно обширного спектра угроз информационной безопасности, дальнейшее развитие которых может повлечь за собой не только потерю конкурентоспособности предприятия на рынке, но и к банкротству и свертыванию бизнеса. Признание серьезности данной проблемы дало толчок к созданию систем для обеспечения информационной безопасности.

Экономическая деятельность предприятия неразрывно связана с финансовой информацией, которая отражает процессы производства, распределения, обмена и потребления материальных благ и услуг. Экономическая информация содержит в себе важнейшую для производства учетную информацию, которая дает характеристику деятельности фирмы за определенный период в прошлом. Основываясь на учетных данных, которые отражают совершившиеся факты хозяйственные деятельности, действия, события, можно скорректировать планы по дальнейшей работе организации,

сделать анализ экономических операций, принять решения по более рациональному распределению работ и т.д. На практике к учетным данным организации относят: информацию бухгалтерского учета, статистическую информацию и информацию оперативного учета. Ее разделяют на оперативную, бухгалтерскую и статистическую информацию. На долю учетной информации приходится более 70% общего объема экономической информации.

Под защитой учетной информации понимается состояние ее защищенности от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям этой информации. [4]

Для учетных данных характерны следующие свойства:

– Огромное разнообразие информации, ее источников, потребителей и большие объемы;

– многократное воспроизведение циклов, крупные массивы вычислений с определенной периодичностью, выполняемые по типовым алгоритмам; (месяц, квартал, год);

– относительно простые арифметические вычисления при большом объеме и сложности логических операций

– "сжатие" информации при продвижении ее вверх. Так, аналитический учет в бухгалтерии ведется в разрезе объектов, как в количественных, так и в стоимостных показателях

– Хранение в течение длительного промежутка времени некоторых результатов и отчетов.

Данные характеристики и свойства обуславливают появление большого числа умышленных хищений конфиденциальной учетной информации, ее искажение, фальсификация и утечка «третьим лицам».

В зависимости от источника угроз их можно разделить на внутренние и внешние. К внешним угрозам можно отнести:

– Локальные, причиной которых могут быть нарушения обязанностей персонала, невнимательность, либо проникновение третьих лиц на территорию организации и получение ими доступа к конфиденциальной информации путем кражи носителей, подключения к ЭВМ или локальной сети;

– Удаленные, характерные для систем, подключенных к глобальным сетям (Интернету, системе международных банковских расчетов SWIFT и др.) [4].

К внутренним относятся действия, связанные с работой персонала:

– Нарушения установленных правил эксплуатации и использования каналов связи для передачи информации, систем обработки и хранения данных.

– Низкий профессионализм и недисциплинированность персонала, халатное отношение к своим обязанностям.

Не менее актуальны проблемы защиты от некачественной информации, поступающей на предприятие извне. Например, руководство организации получает недостоверную информацию о реальном состоянии дел на рынке из-за спланированной и проведенной конкурентами информационной атаки. Предпринятые действия в результате анализа сомнительных данных с большой вероятностью могут привести к принятию ошибочных решений и существенному ущербу состоянию предприятия.

Чтобы обеспечить слаженную работу системы управления компании, необходимо гарантировать эффективное функционирование информационной системы, которая в свою очередь, может предоставить:

– конфиденциальность информации, критически важной для организации или для принятия решения;

– целостность информации и связанных с ней процессов;

– оперативную доступность к различной информации в любой момент времени;

– возможность накопления и сохранности информации;

– минимизацию информационных рисков путем выполнения компенсационных мероприятий и др. [2]

Защиту учетных данных организации также обеспечивают и меры, принятые на законодательном уровне, например, глава 28. Преступления в сфере компьютерной информации (ст. 272-274.1) УК РФ:

– Неправомерный доступ к компьютерной информации (ст. 272);

– Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273);

– создание, использование и распространение вредоносных программ для ЭВМ (ст. 273);

– Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274) [1].

Раскрывает проблему взглядов на обеспечение национальной безопасности в информационной сфере Доктрина информационной безопасности Российской Федерации от 05.12.2016г, а правила ведения учетной информации содержатся в ГОСТах и Федеральный законе Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации.

В безопасности информации различают три классические угрозы для защищенности информации, которые представлены на рисунке 1:

Рис.1 Классические угрозы информационной безопасности [4]

Число рисков, которые повышают уязвимость учетной информации организации, достаточно обширно. Однако, для эффективного предотвращения нарушения конфиденциальности и сохранения безопасности, по нашему мнению, стоит обратить внимание на самые распространенные из них:

– Искажение данных отчетности, размещенной на сайте компании, распространение фальсифицированной документации в сети Интернет;

– Создание фальшивых сайтов организаций [2]

– атаки компьютерными вирусами;

– халатное и недобросовестное отношение к работе персонала, самовольное оставление рабочего места, низкая квалификация работников безопасности;

– неправильный подбор персонала, нечеткое распределение обязанностей, вследствие чего один работник выполняет несколько сложных и объемных задач;

– отказ от дублирования данных, программ и конфиденциальной информации;

– неограниченный доступ к ресурсной базе, компьютерам, на которых хранится учетная информация, сотрудникам, не связанными с работой по ведению, учету и обеспечению информационной безопасности;

– отсутствие контроля за процессом корректной работы программного обеспечения, правильностью выполняемых операций, работой ЭВМ.

Мы считаем, что обеспечение защиты учетной информации является приоритетным направлением в поддержании стабильности экономической безопасности организации. Чтобы избежать кражи, утечки и копирования третьими лицами конфиденциальных данных, необходимо обеспечить максимальную защиту этих данных посредством повышения внимания к таким аспектам, как:

– обеспечение идентификации - аутентификации пользователя;

– определение для каждого пользователя функциональные права — права на выполнение тех или иных функций системы (в частности, на доступ к тем или иным журналам регистрации документов);

– подтверждение авторства пользователя с помощью механизма электронной подписи;

– обеспечение конфиденциальности документов путем их шифрования, а также шифрования всей информации, передающейся по открытым каналам связи (например, по электронной почте); шифрование производится с использованием сертифицированных криптографических средств;

– протоколирование всех действия пользователей в журналах аудита (в журнале аудита входа и выхода из системы, журнале совершенных операций)

– контроль за обеспечением целостности информации и связанных с ней процессов (контроль за процессом работы системы, ПО и т.д.);

– дублирование и хранение конфиденциальных данных на значительном расстоянии от центра обработки;

– регулярная проверка надежности работы компьютера, обновление системы безопасности и антивирусной системы;

– обеспечение установления подлинности и целостности документальных сообщений при их передаче по каналам связи;

– рассмотрение возможности перехода на широко используемый в мире открытый стандарт обмена деловой информацией – язык XBRL. Он позволяет выражать с помощью семантических средств общие для участников рынка и регулирующих органов требования к представлению бизнес-отчётности. Эта система позволяет снизить материальные и временные затраты на обработку большего массива финансовой статистики и уменьшает возможность человеческих ошибок. Данная система широко применяется за рубежом.

На основании проведенного анализа можно сделать вывод, что обеспечение безопасности для учетной информации на предприятии должно являться приоритетным направлением для любой организации, так как от целостности и конфиденциальности данных зависит дальнейшее развитие компании. Должная защита поможет предотвратить дальнейшие риски и угрозы для деятельности организации и более рационально использовать ее потенциал для успешной работы в будущем.

**Библиографический список:**

1. Уголовный кодекс РФ от 13.06.1996 N 63-ФЗ (ред. от 25.03.2022)
2. Шевелев А.Е. Риски в бухгалтерском деле: учеб, пособие /А.Е. Шевелев, Е.В. Шевелева. - Челябинск: Изд-во ЮУрГУ, 2004. – 304 с.
3. Яричина Г.Ф. Роль бухгалтерского учета в обеспечении экономической безопасности организации / Г. Яричина, О. Ситяева, О. Антонова, А. Скуратова // Известия ДВФУ. Экономика и управление – 2019. - № 3 [Электронный ресурс]. — Режим доступа — URL: https://cyberleninka.ru/article/n/rol-buhgalterskogo-ucheta-v-obespechenii-ekonomicheskoy-bezopasnosti-organizatsii/viewer (дата обращения 28.05.2022)
4. Ясенев В.Н. Информационные системы и технологии в экономике / В.И. Ясенев. – М.: ЮНИТИ-ДАНА, 2017. – 560 с.

*Оригинальность 87%*