УДК 657

ЗАЩИТА УЧЕТНОЙ ИНФОРМАЦИИ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Смертенкин М.В., студент гр. ЭУб-161, IV курс
Научный руководитель: Тюленева Т.А., к.э.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

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.

Обеспечение стабильного и максимально эффективного функционирования и развития любого предприятия является основной задачей безопасности экономической информации. Самой ценной экономической информацией является учетная информация, которая характеризует все аспекты хозяйственной деятельности [1; 2]. Сегодня большинство субъектов хозяйствования используют компьютерную форму бухгалтерского учета, которая предполагает использование специализированного программного обеспечения и технических средств. При этом в компьютерных системах формируются, хранятся и обрабатываются большие объемы учетной информации, любой сбой может привести к чрезмерным расходам, недостаточных доходов, потери активов, санкциям. Поэтому главным приоритетом защиты учетной информации на предприятии является разработка мероприятий, направленных на сохранение информации, содержащейся в компьютерных базах предприятия.

В связи с тем, что в последнее время увеличивается количество незаконных финансовых операций, краж и мошенничества в сети Интернет, несанкционированного использования или модификации программного обеспечения, при оценке надежности систем информационной безопасности должны быть изменены приоритеты от обеспечения традиционной информационной безопасности к кибербезопасности.

Вопросы кибербезопасности затрагивают интересы не только государственных институтов, но и коммерческого сектора и гражданского общества. При этом низкий уровень взаимодействия органов государственной власти, неправительственных организаций и коммерческого сектора, а также отсутствие системных нормативных документов, которые описывали бы угрозы в киберпространстве, является следствием отсутствия целостного обсуждения данных вопросов.

Под защитой учетной информации понимается состояние ее защищенности от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут привести к причинению ущерба владельцам или пользователям этой информации. Специалисты по компьютерной безопасности считают, что кибербезопасность – это только новый термин, который определяет именно то, чем они занимались в течение последних десятилетий. Другой научный взгляд на сущность кибербезопасности означает наступательные действия, то есть кибербезопасность отличается от традиционной информационной безопасности тем, что она включает применение практических действий и средств для атаки противников.

Вопросы кибербезопасности должны быть в повестке дня каждого предприятия независимо от его масштабов, уровня сложности и характера коммерческой деятельности, а также осознаны всеми собственниками предприятия. Основным способом предупреждения киберугроз является внедрение последовательных уровней контроля доступа к сайту, системе и файлам. Создание механизма подотчетности позволяет определять, кто работает в системе и что делает в определенный момент времени, и протоколировать события, происходившие в компьютерной информационной системе бухгалтерского учета. Некоторые средства защиты предусматривает программное обеспечение бухгалтерского учета. Так, в программных продуктах "Парус", "1С: Предприятие" имеется возможность формирования пароля для входа в программу, разграничения доступа к функциям и файлам, к отдельным областям учета, установления паролей пользователей, фиксирование авторства созданных документов, ведение журнала регистрации работы с программой, определение прав на удаление документов и записей из информационной базы.

Кроме применения средств защиты в программном обеспечении, должен быть предусмотрен ряд административных мер, например, слежение за отсутствием подслушивающих устройств в компьютерных сетях и тому подобное. При этом важными составляющими защиты являются компетентность и строгое выполнение обязательств по гарантиям соблюдения необходимых правил безопасности учетного персонала, от корректности действий которого зависит уровень кибербезопасности предприятия.

Некомпетентными действиями работников, которые являются угрозой потери информации, являются [3]:

– открытие на своем компьютере файлов, отправленных по электронной почте или программ мгновенного обмена сообщениями от неизвестных адресатов;

- установление нелицензионного программного обеспечения, не нужного для выполнения функциональных обязанностей работника;

- использование паролей "по умолчанию", создание простых паролей или нежелание изменять пароли в течение длительного времени, «запоминание» пароля в окнах ввода, особенно на компьютерах для публичного доступа;

– работа с конфиденциальными документами в местах публичного доступа;

- уведомления по телефону о любых данных об учетной записи, логинах, паролях;

– нецелевое использование сетевых ресурсов и др.

Очевидно, что объектом заинтересованности злоумышленников была и всегда будет частная информация, утечки которой осуществляют при использовании социальных сетей через такие каналы, как персональные компьютеры, ноутбуки, смартфоны, а потому предприятиям необходимо разработать правила пользования этой информацией и следить за безусловным их исполнением.

Эффективность системы кибербезопасности зависит от эффективного управления рисками. В целом управление кибербезопасностью является частью общей системы управления экономической безопасностью предприятия, и в зависимости от размеров и мощности предприятия, а также согласно расчетам экономической ценности защиты учетной информации решаются организационно-кадровые вопросы. Они предусматривают создание или специальной службы по обеспечению кибербезопасности или введение должности специалиста по кибербезопасности, который будет заниматься разработкой охранных систем для разных коммуникационных сетей и электронных баз данных в структуре службы внутреннего контроля предприятия или бухгалтерской службы [4]. Спецслужбу по кибербезопасности могут составлять специалисты по организации информационной безопасности и проведения тестирования на проникновения, инспекторы по организации защиты секретной информации, аналитики проектов по кибербезопасности, системные администраторы, администраторы компьютерных сетей, менеджеры систем информационной безопасности, аналитики систем обеспечения кибербезопасности.

Обязанностями таких специалистов могут быть:

– выявление уязвимых мест системы и моделирование возможной ситуации кибератак с позиции угроз и связанных с ними рисков;

– контроль надежности функционирования системы защиты учетной информации, разработка мер безопасности на случай непередаваемых событий;

– отнесение учетной информации к категории ограниченного доступа (служебной и коммерческой тайн, другой конфиденциальной информации);

– разработка положений, политики и процедур в рамках системы безопасности учетной информации;

– внедрение разработанных мер безопасности и испытания системы с оценкой ее результативности, при необходимости внесение корректировок;

– установление пользователям компьютерной системы бухгалтерского учета необходимых реквизитов защиты;

– обучение пользователей компьютерной информационной системы правилам непрерывной обработки информации;

– контроль за соблюдением пользователями компьютерной информационной системы и персоналом предприятия установленных правил работы с учетной информацией.

В учетной политике предприятия на основе анализа современного уровня развития информационных технологий необходимо рассматривать систематизированное изложение целей, задач и принципов достижения нужного уровня кибербезопасности учетной информации предприятия. При этом стоит помнить, что успешная киберзащита требует затрат.

Таким образом, в отличие от традиционных форм защиты, где упор делается на физическом ограничении, действенность киберзащиты может больше зависеть от обмена информацией, сотрудничества и координации. Это все – вещи, которые трудно поддаются физическому измерению. При этом киберпреступность постоянно совершенствуется и идет в ногу с технологиями, что затрудняет выявление и противодействие указанным противоправным действиям. Поэтому 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 первоочередным фактором, который способствует защите ценной учетной информации. Поэтому на каждом предприятии должна быть создана программа определенных действий, направленных на формирование киберзащиты учетной информации, сфера применения которой распространяется на человеческие ресурсы и не ограничивается исключительно технологическими аспектами.

Список литературы:

1. Raiding as a treat to economic security of Kuzbass coal mining enterprises / Tyuleneva T.A. // В сборнике: E3S Web of Conferences Electronic edition. 2018.

2. Improvement of measures to counteract raider acquisition of Kuzbass coal mining enterprises / Tyuleneva T.A. // В сборнике: E3S Web of Conferences Electronic edition. 2018.

3. Клименко В. Внутрішні загрози інформаційній безпеці організації / В. Клименко // Вісник НБУ. 2008. № 5. С. 62-63.

4. Витер С.А., Светлишин И.И. Защита учетной информации и кибербезопасность предприятия. Економіка і суспільство, 2017. № 11. С. 497-502.