

# СПЕЦИАЛЬНАЯ ДИСЦИПЛИНА «БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БИЗНЕСА»

*Е.Н. Ливак*

УО «Гродненский государственный университет имени Янки Купалы»,  
кафедра интеллектуальных и компьютерных технологий  
ул. Ожешко, 22, г. Гродно, Республика Беларусь  
телефоны: +375296518722; 80152730305; e-mail: livak@grsu.by; web: mf.grsu.by

Представлена разработанная автором специальная дисциплина (спецкурс) «Безопасность электронного бизнеса». Обоснована целесообразность изучения спецкурса будущими IT-специалистами, рассмотрены основная тематика и направленность.

**Компьютерная безопасность, электронный бизнес.**

## 1 ЦЕЛЕСООБРАЗНОСТЬ ИЗУЧЕНИЯ

Коммерческая, управленческая и экономическая деятельность человека претерпели фундаментальные изменения под влиянием информационных технологий. «Любая технология рано или поздно становится технологией информационной (ИТ): если не целиком, то по крайней мере отдельные ее компоненты имеют отношение к ИТ, а если еще не имеют, то в скором времени будут. Вся наша жизнь – бизнес, системы управления, культура – проходят под знаком ИТ» [1]. Новейшие информационные технологии обеспечивают как новые источники, новые методы доставки и обмена информацией, так и новые способы манипуляции информацией, продолжая изменять характер сделок и других операций в бизнесе. Телекоммуникационные технологии изменили и продолжают совершенствовать методы ведения бизнеса.

Для современного высококвалифицированного специалиста в любой области становятся все более важными навыки управления бизнес-информацией как ресурсом и товаром, навыки эффективного использования ИТ для повышения производительности и получения конкурентных преимуществ.

В наши дни считаются эффективными способы вести дела с помощью технологий электронного бизнеса и электронной коммерции. Тысячи компаний во всем мире применяют информационные компьютерные технологии для ведения бизнеса. Деловые операции проводятся в электронном виде. Крупные компании используют Web-сайты, корпоративные порталы и торговые электронные площадки (e-MarketPlaces) – интерактивные электронные каталоги, электронные биржи, корпоративные и потребительские аукционы, сообщества, торговые информационные системы – как дополнительное (а иногда и основное) средство сбыта и продвижения товаров. Мелкие и средние компании проводят электронные маркетинговые мероприятия и занимаются электронной коммерцией в

Internet. Создаются и развиваются электронные виртуальные предприятия. Широкое распространение получают электронные торговые и посреднические центры. Привычной и прибыльной становится Internet-реклама, разрабатываются новые технологии электронной рекламы. Развивается электронный менеджмент. Управление предприятием становится немыслимым без автоматизированных систем управления, а принятие управленческих решений – без компьютерного интеллектуального анализа специальным образом организованных и структурированных данных. Системы планирования ресурсов предприятия (ERP-системы), системы управления взаимоотношениями с клиентом (CRM) становятся неотъемлемой частью информационной инфраструктуры предприятий. Все шире внедряются BPM-системы (Business Process Management System) как программный инструментарий для управления бизнес-процессами предприятия.

Сегодня национальные и глобальные инфраструктуры, обеспечивающие электронный перевод денежных средств, авторизацию кредитных и дебетовых карт, поддерживают финансовые операции на миллиарды долларов, и этот показатель растет в геометрической прогрессии. Электронное управление банковским счетом посредством систем «Банк-Клиент» становится привычным не только для юридических, но и для физических лиц. Особое место в современном мире занимают созданные банками и другими финансовыми структурами электронные платежные системы, позволяющие осуществлять удаленные платежи с помощью электронных денег.

Главная проблема, сдерживающая не только широкое применение удаленных Internet-платежей посредством электронных денег, но и в целом развитие электронной коммерции и электронного бизнеса – уровень обеспечения безопасности информационных технологий, являющихся современными инструментами электронного бизнеса. Уровень эксплуатационной надежности применяемых систем и технологий электронного бизнеса, целостности, доступности и конфиденциальности обрабатываемой информации сегодня не в полной мере отвечает требованиям реального бизнеса.

Более того, безопасность многими специалистами признается ключевым вопросом для внедрения и широкого применения большинства инструментальных программных средств электронного бизнеса. Именно психологические факторы, связанные с объективной информированностью и осознанием обществом угрозы потенциального

мошенничества (раскрытие персональных данных и мошеннические финансовые транзакции, совершенные с помощью украденных данных), с возможными конфликтами между покупателями и электронными торговыми предприятиями, клиентами и банками, препятствуют реализации широкомасштабных проектов в области электронного бизнеса.

Однако те многочисленные преимущества, которые предоставляют и могут предоставить в будущем средства и системы поддержки электронного бизнеса, накопленный мировой опыт в обеспечении необходимого уровня безопасности проведения бизнес-транзакций позволяют утверждать, что широкомасштабное внедрение средств электронного бизнеса будет продолжаться и стимулироваться.

Проведенный анализ тенденций и прогнозов развития информационно-коммуникационных технологий во всем мире позволяет назвать перспективными технологии автоматизации бизнеса, а технологии безопасности электронного бизнеса – стратегическими.

Именно поэтому, с точки зрения автора, высокопрофессиональный IT-специалист и особенно специалист в области защиты информации обязан не только теоретически владеть современными технологиями электронного бизнеса, иметь практические навыки по использованию средств e-business, но и владеть средствами защиты бизнес-информации, коммуникаций и транзакций; быть компетентным в области обеспечения безопасности современных электронных бизнес-технологий (профессиональное администрирование); разрабатывать новые технологии безопасности.

«В виртуальном мире нет рукопожатий», поэтому защита от мошенничества и злонамеренных действий в системах электронного бизнеса – задача, которую необходимо решать IT-специалистам.

Автором был разработан и на протяжении пяти лет читался студентам специальный курс «Электронный бизнес». Полученный опыт, а также тенденции и проблемы развития средств и технологий электронного бизнеса стали теми факторами, которые стимулировали разработку новой специальной дисциплины – «Безопасность электронного бизнеса».

## 2 ОСНОВНАЯ ЗАДАЧА И ЦЕЛЬ СПЕЦКУРСА

Основная задача спецкурса – сформировать фундаментальные знания и компетенции студентов в области обеспечения безопасности технологий электронного бизнеса.

Цель спецкурса – ознакомить слушателей с принципами работы систем e-commerce и e-business, технологиями безопасности электронного бизнеса, научить слушателей эффективно применять на практике современные методы, механизмы и средства защиты бизнес-информации, увеличивать производительность, получать конкурентные преимущества и выгоду от широких возможностей современных электронных бизнес-технологий.

## 3 ОСНОВНАЯ НАПРАВЛЕННОСТЬ И ТЕМАТИКА

Спецкурс предназначен для студентов, уже владеющих основами защиты компьютерной информации от несанкционированного доступа и нелегального использования, а также основами защиты глобальных и локальных сетевых технологий.

Электронный бизнес автором рассматривается как все стороны деловых отношений в Internet/intranet: продажи, маркетинг, финансовый анализ, платежи, поддержка партнерских отношений, поиск сотрудников, автоматизация коллективной работы и делопроизводства и подчеркивается, что основная тяжесть поддержки электронного бизнеса ложится на безопасное и надежное программное и аппаратное обеспечение и каналы связи.

Один из важнейших изучаемых модулей – «Обеспечение безопасности электронных платежей с помощью банковских карт и электронных денег». На основе систематизации знаний в области криптографической защиты данных (алгоритмы шифрования, коды аутентификации сообщений, функции хэширования, системы формирования и проверки электронной цифровой подписи, электронные ключи), знакомства с системами управления ключами и основными протоколами и средствами защищенного обмена данными изучаются: стандарты и принципы безопасности электронных расчетов, протокол SSL (Secure Socket Layer), стандарт SET (Secure Electronic Transaction), стандарт 3D Secure. Методы обеспечения безопасности платежей в системах электронной наличности рассматриваются на примерах (сравнительный анализ) российских систем электронной наличности PayCash (Яндекс.Деньги) и WebMoney Transfer, официальной системы микроплатежей через Internet в Беларуси EasyPay и платежной системы E-Gold.

При изучении модуля «Обеспечение безопасности работы электронных торговых площадок и предприятий» рассматриваются основные методы и средства защиты серверов электронной коммерции и электронных транзакций; защита от несанкционированного доступа и модификации контента корпоративных web-сайтов, а также основные угрозы безопасности Internet-магазинов (web-витрин) и торговых Internet-систем, средства обнаружения атак, способы обнаружения мошенничества.

В рамках спецкурса рассматриваются и другие модули, например, модуль по изучению современных технологий частного электронного бизнеса с целью ознакомления слушателей с различного рода мошенничествами под девизом «Как заработать деньги в Internet?»

## ЛИТЕРАТУРА

- [1] Информационные технологии в бизнесе / Под ред. М. Желены. – СПб: Питер, 2002. – 1120 с.