Вестник ТвГТУ. Серия «Науки об обществе и гуманитарные науки». 2021. № 3 (26). С. 68–76

ПРОБЛЕМЫ ЭКОНОМИКИ И УПРАВЛЕНИЯ

УДК 657.6.012.16

МЕТОДОЛОГИЯ ФОРЕНЗИКИ В ИССЛЕДОВАНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Т.Б. Яконовская

ФГБОУ ВО «Тверской государственный технический университет», г. Тверь

DOI:10.46573/2409-1391-2021-3-68-76

В статье проанализированы основные виды экономических преступлений, совершаемых с помощью информационных технологий. Показана взаимосвязь экономической и информационной безопасности предприятия. Рассмотрены методология форензики и применение ее инструментария в антикризисном менеджменте, а также в области экономической безопасности предприятия. Исследованы инструменты, обеспечивающие проведение криминалистического анализа и сбора информационных доказательств.

Ключевые слова: *форензика, компьютерная криминалистика, экономическая безопасность, информационная безопасность, экономические преступления, киберпреступления.*

В современной научной экономической литературе большое внимание уделяется вопросам оценки уровня экономической безопасности предприятия. Нет единого мнения по поводу того, что понимать под термином «экономическая безопасность». Одни ученые утверждают, что экономическая безопасность характеризуется финансовым состоянием предприятия, поэтому для оценки уровня рассматриваемой безопасности достаточно провести глубокий финансовый анализ. Другие считают, что экономическая безопасность – это комплексное понятие, включающее не только финансы, но и организационно-технический, кадровый, экологический, юридический и информационный элементы, а потому для диагностики экономической безопасности предприятия необходимо исследовать каждый ее структурный элемент с помощью различных научных инструментов [3; 9; 10].

В эру цифровой трансформации экономики самым главным активом любой организации становится информация, поэтому известная фраза «кто владеет информацией, тот владеет миром» становится весьма актуальной. Если предприятие хочет «владеть миром» (его стратегическая цель заключается в усилении своих конкурентных рыночных позиций, развитии и захвате рынков), то оно не только должно «владеть информацией», но и уметь ее защищать. Следовательно, вопросам и методам защиты и анализа коммерческих сведений предприятие должно уделять особое внимание.

Бурное развитие информационных технологий и их внедрение в повседневную хозяйственную деятельность организаций и граждан приводят иногда к тому, что эти технологии применяются в преступных целях. Так, по данным правовой статистики [3], более 70 % экономических преступлений в

России совершается с помощью информационных технологий (рис. 1). Этот процент из года в год растет.

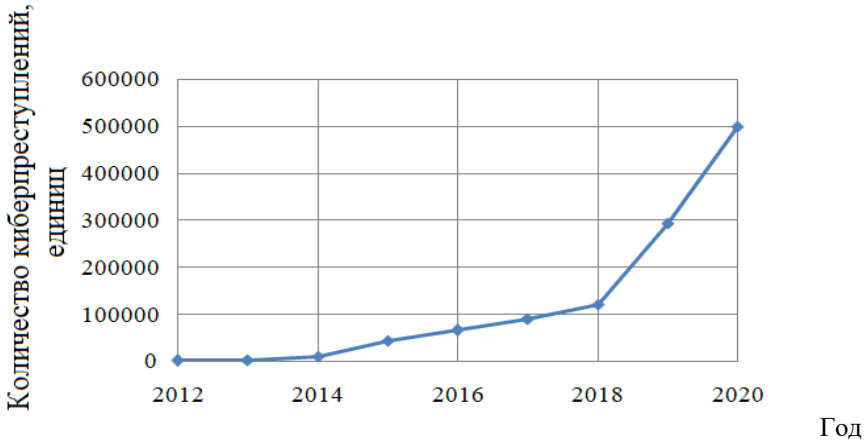

Рис. 1. Динамика экономических преступлений
с использованием IT-технологий в РФ

Понятие «экономические преступления, совершаемые с использованием информационных технологий» – это комплексный термин. Многомерность понятия обусловлена обилием видов преступлений экономического характера, совершаемых с использованием информационных технологий (киберпреступлений). Эти преступления, согласно нормам Уголовного кодекса Российской Федерации (УК РФ) [6], ужесточенным в 2011 году, классифицируются следующим образом:

мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

преступления в сфере компьютерной информации (гл. 28 УК РФ);

неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Однако Управление Министерства внутренних дел (УМВД) по Тверской области начало вести аналитику в отчетах о киберпреступлениях только с 2016 года (рис. 2) (напомним, что необходимость отчета была закреплена в федеральном законе еще в 2011 году). Дисциплина регистрации таких преступлений низкая [7; 11]. Так, например, до 2020 года учету подлежали только два вида киберпреступлений: дистанционные мошенничества, при которых применяются различные механизмы хищения денег с банковских карт, и мошенничество с использованием сети Интернет и средств мобильной связи. Отметим, что в отчете за 2020 год появился новый вид киберпреступления, не зафиксированный новыми нормами УК РФ. Его можно назвать гибридным: это преступление, связанное с незаконным оборотом наркотиков и осуществляемое с помощью мобильного телефона. Так, по Тверскому региону в 2020 году было

зафиксировано 279 случаев подобных преступлений. Отметим также факт небрежного статистического учета киберпреступлений: в ежегодном отчете упомянутого нами УМВД имеется ряд несоответствий и опечаток, что недопустимо, так как именно этот источник статистических данных является официальным и от достоверности указанной в нем информации зависит точность последующей аналитики (табл. 1).

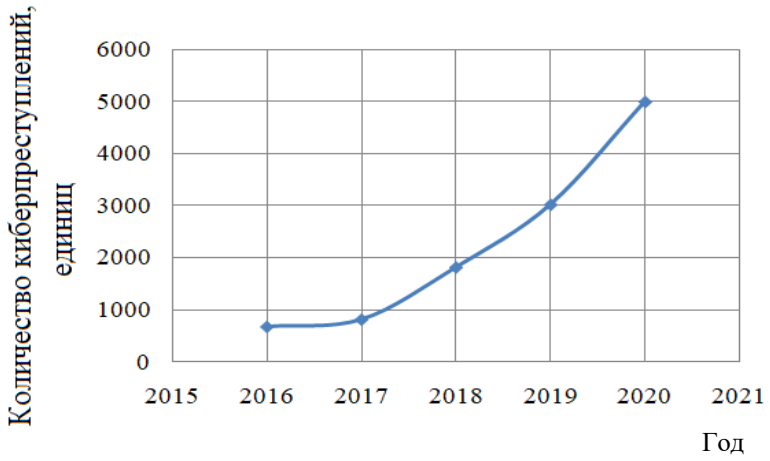

Рис. 2. Статистика количества киберпреступлений по Тверскому региону

Таблица 1

Статистика данных о киберпреступлениях по Тверскому региону*

Вид киберпреступления по УК РФ	Год				
	2016	2017	2018	2019	2020
Всего по региону	677	817	1819	3022 (3701)	4997 (4300)
Дистанционные мошенничества, хищения денег с банковских карт	92	151	294	771	2158
Мошенничество с использованием сети Интернет и средств мобильной связи	585	666	1597 (877)	2930	2142
Среднее число киберпреступлений в день, случаев	(–)	(–)	(–)	7	(–)
Число зарегистрированных обращений, ед.	140	152 (151)	282	(–)	(–)*

Примечания:
1. * – несоответствие данных в ежегодных официальных отчетах УМВД.
2. (–)* – данные отсутствуют в официальном отчете УМВД.

Анализ информации, представленной на рис. 2, показывает, что темп роста преступлений с использованием IT-технологий из-за внедрения идеологии цифровой экономики резко возрос (с 2017 года). В целом по Тверскому региону доля киберпреступлений в 2020 году в общем объеме преступлений достигла 23 %, причем преобладают кражи с банковских счетов граждан (2158 случаев (43,2 %)) и мошенничества (2142 случая (42,8 %)). Киберпреступных

посягательств экономической направленности других видов зафиксировано 155 случаев (3,1 %).

Следует отметить, что особенностью киберпреступлений является крайне низкая и неэффективная раскрываемость.

Как правило, преступления с применением IT-технологий следователи делят на два типа (в зависимости от вида пострадавших):

1) совершенные в отношении физических лиц (граждан);

2) совершенные в отношении юридических лиц (организаций, предприятий).

На практике учет и статистика первого типа киберпреступлений осуществляются медленно, расследуются эти преступления только после того, как ущерб по ним позволит перевести их в разряд преступлений средней тяжести или тяжелых.

Как правило, кибермошенничество в отношении физических лиц чаще всего представляет собой перевод денежных средств с личных банковских счетов на счет мошенника. При осуществлении такого хищения используют мобильный телефон и поддельный сайт банка, в котором размещены финансовые средства человека (пример такого рода интернет-страницы дан на рис. 3). В настоящее время кибермошенничеством занимаются примерно 130 различных группировок. Их количество ежегодно растет.

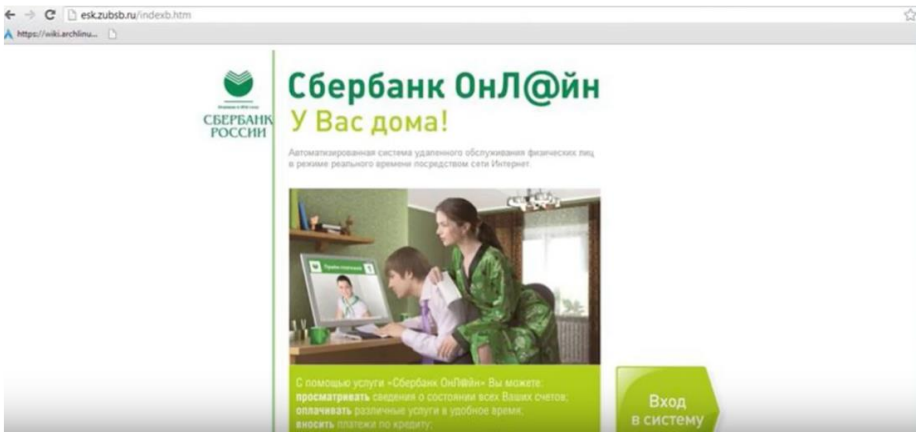

Рис. 3. Пример сайта, сделанного мошенниками и похожего на сайт Сбербанка

Наказание за описанный выше способ кибермошенничества – это либо штраф (минимум 100 тыс. руб.), либо принудительные работы (от 1,5 до 5 лет), либо ограничение свободы (до 7 лет), либо сочетание перечисленных вариантов. Проблема низкой раскрываемости такого типа киберпреступлений связана не только с несовершенством законодательства в этой сфере, но и с отсутствием навыков, знаний, технологий и средств для их раскрытия. В лучшем случае наказывается помощник кибермошенника, снимающий переведенные денежные средства, организатор же уходит от уголовной ответственности. Возникают резонные вопросы: если все движения денежных средств совершаются через банковскую систему, то почему банки не могут обезопасить сбережения, вклады

своих клиентов?; почему бы не скоординировать действия службы безопасности банка и УМВД? К сожалению, именно клиент банка несет убытки. Жертва кибермошенника, помимо перевода на посторонний счет личных средств, может совершить и другие действия, наносящие урон ее материальному благополучию, например взять кредит, который потом тоже переведет мошеннику, а проценты по нему будет платить сама. Возможно, если банки прекратили бы практику одобрения кредита без личного участия и проверки клиента, то ущерб от кибермошенничества был бы минимален, т.е. ограничивался бы потерей вклада, прочего вида отложенных средств, поскольку отсутствует необходимость выплаты процентов по кредиту.

Следует отметить, что в структуре информационно-аналитической записки к ежегодному отчету начальника УМВД по Тверской области присутствует раздел «Результаты мониторинга общественного мнения», в котором отражено отношение населения к деятельности указанной организации (табл. 2, рис. 4). Работе с обращениями граждан по поводу кибермошенничества следует уделять более пристальное внимание, так как количество таких преступлений из года в год увеличивается, причем очень быстро. Это обусловлено прежде всего несовершенством законодательства в сфере киберпреступности.

Таблица 2

Статистика оценки уровня доверия граждан органам внутренних дел Тверской области

Показатель	Год							
	2013	2014	2015	2016	2017	2018	2019	2020
Процент опрошенных граждан, доверяющих работе органов внутренних дел	33	85*	65*	29,59	35,3 (36)*	36,2 (35,5)*	37,8	43

Примечания:

1. * – при составлении использованы данные социологического опроса, проведенного по методике Российского государственного социального университета.
2. (…)* – несоответствие данных в отчете.

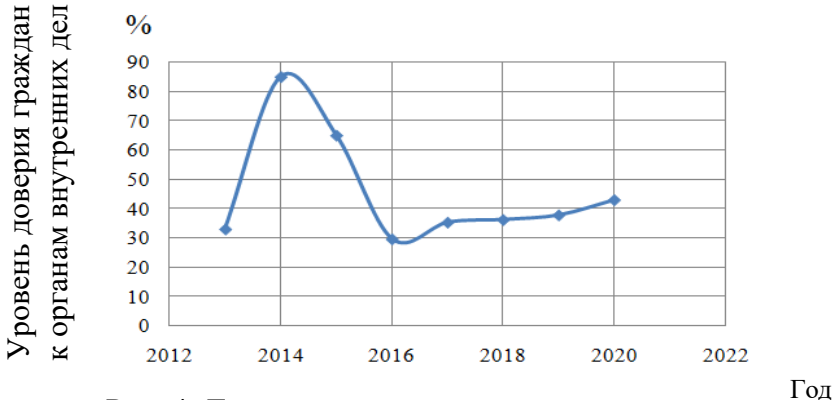

Рис. 4. Динамика уровня доверия граждан к органам внутренних дел Тверской области

В первую очередь обычно расследуют киберпреступления, совершенные в отношении юридических лиц (организаций, предприятий), так как ущерб в данном случае на порядок выше (миллионы, миллиарды рублей) и мгновенно может привести к потере экономической безопасности и банкротству.

Современное предприятие – это цифровая организация, в которой вся документация и информация хранится в электронном виде, а управление бизнес-процессами производится с помощью информационно-телекоммуникационных технологий [4; 10]. При этом из-за внедрения экспертных информационно-аналитических систем на предприятиях со временем исчезнет потребность во многих специалистах (бухгалтере, маркетологе, кадровике и др.): их заменит бизнес-аналитик. Иными словами, любое предприятие представляет интерес для киберпреступников, поэтому для обеспечения экономической безопасности необходимо уделять особое внимание ее информационной составляющей. Здесь важную роль играет форензика.

Форензика (компьютерная криминалистика, расследование киберпреступлений) – это прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. Это довольно молодая наука, являющаяся ответвлением дисциплины «Информационная безопасность», следовательно, она меньше развита, чем тестирование на проникновение или организация защитных средств. Форензика также представляет собой новый вид аудиторских и экспертно-аналитических услуг.

По отношению к предприятию форензика в узком смысле слова может рассматриваться не только как метод выявления финансовых преступлений, но и как инструментарий аудита и ревизии, что показано в работах [1; 2; 5; 8; 10–13]. Однако в этих исследованиях не указано и не описано важное назначение форензики, заключающееся в проведении финансового следствия по сбору цифровых доказательств, которые затем могут использоваться в суде по делу о банкротстве.

Методологию форензики часто применяют при прохождении предприятием процедур банкротства. В этом случае антикризисный управляющий – это своего рода финансовый следователь (детектив), имеющий в своем арсенале методы компьютерной криминалистики, бухгалтерского учета и аудита, финансового и экономического анализа, психологии для диагностики преднамеренного банкротства, выявления подозрительных сделок с финансами и собственностью, а также легализации доходов, полученных незаконным путем, и т.д. Иными словами, антикризисный менеджмент включает в себя методы и приемы форензики, направленные на диагностику любого рода кризисных ситуаций, возникающих на предприятии, а также мероприятия по профилактике кризисов, адаптации и сглаживанию негативных экономических тенденций. Связь процедур банкротства с форензикой показана в табл. 3.

Таблица 3

Использование методов форензики на стадиях банкротства предприятия

Стадия банкротства предприятия	Метод форензики
Наблюдение	Бизнес-разведка – проверка репутации контрагентов, финансовое расследование, поиск активов, выявление преднамеренного банкротства (компьютерная криминалистика, IT-форензика)
Финансовое оздоровление	Защита собственности, в том числе интеллектуальной
Внешнее управление	Управление рисками мошенничества, противодействие легализации незаконных доходов, интеллектуальный анализ данных для предупреждения мошенничества, мониторинг подозрительных операций, IT-форензика
Конкурсное производство	Финансовое расследование, поиск активов, интеллектуальный анализ данных для предупреждения мошенничества, мониторинг подозрительных операций, экспертиза, IT-форензика
Мировое соглашение	–

Кроме того, методологию и инструментарий форензики можно использовать и в повседневной работе организации для оптимизации и мониторинга расходов и доходов, а также профилактики кризисных ситуаций и оценки несанкционированных входов в информационную систему фирмы. На практике чаще всего кибератакам подвергается информационно-телекоммуникационная сеть предприятия, поэтому основными направлениями аналитики в форензике являются:

1. Computer forensics – компьютерная криминалистика систем ЭВМ; исследование хоста и локальной сети, файловой системы, оперативной памяти и др.

2. Forensic data analysis – компьютерная криминалистика файлов и программ, обнаружение и исследование вредоносных программ под различные операционные системы (Windows, macOS, Solaris, Linux и пр.) и т.д.

3. Mobile forensics – компьютерная криминалистика мобильных устройств; исследование действий владельца мобильного телефона, работающего под управлением многих операционных систем: Android, KaiOS, LineageOS, Fire OS, Flyme OS, iOS, Sailfish OS, Tizen, Remix OS и т.п.

4. Network forensics – криминалистика компьютерных сетей; исследование проходящего трафика узлов сети на наличие угроз кибератаки по сети и др.

5. Hardware forensics – компьютерная криминалистика аппаратно-программного обеспечения; исследование микроконтроллера, прошивки аппаратного устройства и т.д.

Чаще всего результатом несанкционированного входа в операционную систему на предприятиях является кража экономической информации, которая может привести к катастрофическим для фирмы последствиям. Например, у ООО «Мелиосервис» в 2011 году была похищена клиентская база, в результате чего предприятию был нанесен ущерб, который привел к ликвидации организации. Хищение клиентской базы – весьма распространенное преступление, доказать

которое очень сложно. В приведенном примере (случай с ООО «Мелиосервис») использовался следующий инструментарий из арсенала форензики для выявления несанкционированных попыток входа в систему предприятия Linux:

1. Анализировали журнал безопасности операционной системы Linux.

2. Применяли специализированные программно-аппаратные средства, такие как жесткий диск, контроллер, операционная оболочка, драйверы (файловая система), специализированные программы для просмотра содержимого файлов (к примеру, «less»), драйвер видеоплаты, средства ввода и вывода информации и их программы. В результате получили запись о попытках несанкционированного входа в операционную систему Linux (рис. 5).

Рис. 5. Пример искажения неудачных попыток входа в систему Linux

Для пресечения хищений экономической информации, кибератак вредоносными программами, а также удаленного незаконного управления активами организации необходимо обучать технических специалистов предприятия методам первичной фиксации цифровых доказательств.

Библиографический список

1. Аблязова С.А. Форензик как инструмент финансового расследования деятельности организаций // Ученые записки Крымского инженерно-педагогического университета. 2020. № 1 (67). С. 20–23.
2. Городилов М.А., Шкляева Н.А. Форензик в рамках экспертно-аналитической и аудиторской деятельности: теоретическое исследование понятия // Учет. Анализ. Аудит. 2018. Т. 5. № 2. С. 72–79. DOI: 10.26794/2408-9303-2018-5-2-72-7.
3. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий (отчет Генпрокуратуры РФ) [Электронный ресурс]. – Режим доступа: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (дата обращения: 10.05.2021).
4. Палюх Б.В., Борисов А.Л. Основы построения информационных систем. Тверь: ТвГТУ, 2019. 136 с.
5. Пастухов П.С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 450–460.
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». Источник: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 10.05.2021).
7. Управление МВД России по Тверской области [Электронный ресурс]. – Режим доступа: https://69.мвд.рф/action/Otchjoti_dolzhnostnih_lic (дата обращения: 10.05.2021).
8. Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений. М.: Горячая Линия–Телеком, 2019. 104 с.
9. Яконовская Т.Б., Жигульская А.И. Особенности оценки экономической безопасности предприятий торфодобывающей отрасли Тверского региона

России (обзор отрасли) // Горные науки и технологии. 2021. Т. 6. № 1. С. 5–15. DOI: 10.17073/2500-0632-2021-1-5-15.
10. Яконовская Т.Б., Жигульская А.И., Оганесян А.С. Управление структурой активной части основных фондов торфодобывающих предприятий с использованием информационной системы // Актуальные вопросы теории и практики бухгалтерского учета и финансов: материалы II Научно-практической конференции, Тверь, 28–29 апреля 2020 года. Тверь: ТвГТУ, 2020. С. 149–155.
11. Яконовская Т.Б., Зюзин Б.Ф., Жигульская А.И. Оценка эффективности работы главного управления региональной безопасности Тверской области по противодействию коррупции в регионе // Современные технологии и инновации: материалы IV Всероссийской научно-практической конференции, Тверь, 19 марта 2020 года / под общ. ред. Т.Б. Новиченковой. Тверь: ТвГТУ, 2020. С. 54–59.
12. Davis Ch. Characteristics and skills of the forensic accountant [Electronic resource]. – Access mode: http://www.aicpa.org/InterestAreas/ForensicAndValtion/Resources/PractAidsGuidance/DownloadableDocuments/ForensicAccountingResearchWhitePaper.pdf (accessed: 10.05.2021).
13. Freeman Sh. How forensic accounting works [Electronic resource]. – Access mode: http://science.howstuffworks.com/forensicaccounting.htm (accessed: 10.05.2021).
14. Golden T.W., Skalak S.L., Clayton M.M. A guide to forensic accounting investigation. Hoboken, New Jersey: John Wiley & Sons, 2006. 565 p.
15. Weaver L. Forensic auditing [Electronic resource]. – Access mode: http://www2.accaglobal.com/documents/forensic_auditing.pdf (accessed: 10.05.2021).

FORENSIC METHODOLOGY IN ECONOMIC SECURITY STUDIES

T.B. Yakonovskaya

Tver State Technical University, Tver

The article analyzes economic crimes committed with the use of information technology. The relationship between economic security and information security of an enterprise is shown, and the methodology of forensics is considered in the aspect of applying its tools to anti-crisis management and economic security of an enterprise. The tools that provide forensic analysis and collection of informational evidence are being investigated.

Keywords: *forensics, computer forensics, economic security, information security, economic crimes, information technology.*

Об авторе:

Яконовская Татьяна Борисовна – кандидат экономических наук, доцент кафедры экономики и управления производством ФГБОУ ВО «Тверской государственный технический университет», г. Тверь, Россия. SPIN-код: 7769-2901; e-mail: tby81@yandex.ru

Author infotmation:

Yakonovskaya Tatyana Borisovna – PhD (Economic Sciences), Associate Professor of the Department of Economics and Production Management of Tver State Technical University, Tver, Russia. SPIN-code: 7769-2901; e-mail: tby81@yandex.ru