DOI https://doi.org/10.46845/2541-8254-2022-3(35)-7-7

УДК 338.1

АКТУАЛЬНЫЕ УГРОЗЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

Л.В. Черных, студентка 3-го курса,
e-mail: vafleman@gmail.com
ФГБОУ ВО «Калининградский государственный университет»,

В.Б. Горбунова, канд. экон. наук, доцент
e-mail: viktoriya.gorbunova@klgtu.ru
ФГБОУ ВО «Калининградский государственный университет»

В статье исследованы актуальные угрозы обеспечения экономической безопасности в киберпространстве. По мере распространения пандемии, общество и государство столкнулись с еще одной глобальной проблемой в лице серии кибератак и киберпреступлений со стороны компьютерных мошенников, при этом пропорционально росту количества киберпреступлений растет и причиняемый ими ущерб. В работе изложен подход к расчету эффективности мероприятий по повышению уровня кибербезопасности. По результатам анализа обозначены основные направления и возможные методы и способы повышения кибербезопасности в современных условиях. Было выявлено, что только совместными усилиями государства и бизнеса возможно нивелировать угрозы экономической безопасности в условиях расширения киберпространства, которое неизбежно сопровождается выявлением все новых видов кибератак, мошенничества и других информационных преступлений.

Ключевые слова: *кибербезопасность, киберпреступления, мошенничество, кибермошенничество, экономическая безопасность, риски, угрозы, информационные технологии.*

ВВЕДЕНИЕ

На современном этапе развития общества информационные технологии стали невероятно значимы в экономическом секторе. В современном мире невозможно представить жизнь без сети «Интернет», банковских карт и интернет-магазинов. 78 % населения России старше 12 лет используют Интернет, 91 % из них – ежедневно [1]. Ежедневно в сети проводится свыше 25 миллионов денежных операций на сумму более 8 млрд. долларов. В 2020 г. количество заказов составило 830 миллионов, рост по сравнению с 2019 г. – 78 %. Таким образом, встает острый вопрос о безопасности совершения покупок в сети и защите своих личных данных.

Активно получают распространение результаты интеллектуального труда: видео игры, дизайнерские проекты, программные обеспечения, нейронные сети и т. д. Все эти элементы также являются неотъемлемой частью экономической системы и, соответственно, должны быть как следует защищены.

ОБЪЕКТ ИССЛЕДОВАНИЯ

Объектом исследования являются угрозы обеспечения кибербезопасности предприятий и государства в современных условиях.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Цель исследования – выявить актуальные угрозы в киберпространстве, влияющие на экономическую безопасность.

Для достижения поставленной цели был определен ряд задач, требующих решения, а именно:

- изучить основные категории интернет-вмешательств в деятельность предприятий;
- проанализировать возможные угрозы экономической безопасности, связанные с киберпространством и использованием сети Интернет;
- оценить степень киберзащищенности в современных условиях;
- обозначить возможные методы и способы повышения кибербезопасности государства и бизнеса.

МЕТОДЫ ИССЛЕДОВАНИЯ

В процессе написания работы были использованы следующие общенаучные методы исследования: анализ, обобщение, описание, измерение, сравнение.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Безопасность любой системы бизнеса в интернете заключается в защите данных от различного рода вмешательств. [2] Все эти вмешательства можно разделить на несколько категорий, которые представлены на рисунке 1.

Рисунок 1 – Наиболее уязвимые сферы киберпространства

Но более значимой задачей в вопросе защищенности бизнеса в сети считается отставание правовой базы в связи с быстрым развитием технологий и сети «Интернет». Преступника практически невозможно поймать на месте преступления, всевозможные улики или же обличающие данные имеют все шансы быть быстро и просто уничтожены без шансов на восстановление. Этим обусловлена особая значимость совершенствования правовой базы и проработки политики безопасности собственных систем особенно для фирм, основной бизнес которых базируется на онлайн-платформах [3].

Стоит обозначить то, что абсолютная и безоговорочная безопасность невыполнима в современных условиях, так как защитные системы формируются на базах большого количества уже имеющих место быть систем. В том числе и в случае если представить, что такую систему возможно реализовать, нельзя упускать из поля зрения такой важнейший

«нюанс», как человеческий фактор. [4] По большому счету всевозможные защитные системы формируются, видоизменяются и управляются людьми, а согласно исследованиям 81 % респондентов отметили, что наибольшее беспокойство у компаний вызывает именно внутренняя угроза – умышленные или неумышленные действия собственных сотрудников. [5].

Помимо внутренней угрозы в лице сотрудников нельзя не отметить существенные внешние угрозы. Наиболее ярко этот момент можно отследить на примере пандемии SARS COV-2 [6].

По мере распространения пандемии, общество и государство столкнулись с еще одной глобальной проблемой в лице серии кибератак и киберпреступлений со стороны компьютерных мошенников. Длительный стресс, оказываемый на население, многократное увеличение безналичных транзакций привели к появлению тепличных условий для интернет мошенничества.

Поскольку в период пандемии население больше, чем когда-либо в истории, полагалось на компьютерные технологии, интернет и другие подобные устройства и технологии для учебы, работы, совершения покупок, обмена и получения информации.

Таким образом, сейчас стала буквально процветать одна из разновидностей мошенничества – кибермошенничество. Кибермошенничество – это одно из разновидностей киберпреступления, целью которого является хищение конфиденциальной информации пользователя (пароли, номера банковских карт, паспортные данные и т. д.) для получения материальной или иной выгоды.

По данным МВД России, на фоне пандемии коронавирусной инфекции в 2020 г. был замечен резкий рост мошеннических преступлений (ст. 159–159.6 УК РФ). Таким образом, только за первое полугодие были задокументированы 101756 преступлений данного типа. В свою очередь, в 2019 г. было зарегистрировано 257217 преступлений, направленных на мошеннические действия за весь календарный год. Также зарегистрирован колоссальный рост мошенничества с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. В 2020 г. количество случаев кибермошенничества выросло более чем на 82 % в сравнении с 2019 г.[7]. Наиболее уязвимые сферы киберпространства представлены на рисунке 2.

Рисунок 2 – Наиболее уязвимые сферы киберпространства

Пропорционально росту количества киберпреступлений растет и причиняемый ими ущерб. По официальным данным Центрального Банка РФ, потери клиентов банков России от кибермошенничества в 2020 г. исчислялись суммой 9 млрд. руб. Потери в российском сегменте ежегодно составляют около 450 млн. долларов, по данным МВД РФ. Столь ощутимые потери, несомненно, наносят глобальный ущерб экономической безопасности государства.

Исследование, проведенное в 2007 г., показало, что злоумышленники ранее атаковали компьютеры и сети со скоростью одной атаки каждые 39 с. В отчете Центра жалоб на преступления в Интернете за 2020 г. было установлено, что в этом году было зарегистрировано 465 177 инцидентов, что приводит к одной успешной атаке каждые 1,12 с. Примечательно, что при этом не учитывались попытки атак или те из них, о которых не сообщалось [8].

CyberEdge Group проводило исследование в 17 странах, включающих Северную Америку, Европу, Азиатско-Тихоокеанский регион, Ближний Восток, Латинскую Америку и Африку. Согласно полученным результатам в 2021 г. 86,2 % опрошенных организаций пострадали от успешной кибератаки [9]. Динамика количества организаций, подвергшихся по крайней мере одной успешной кибератаке, представлена на рисунке 3.

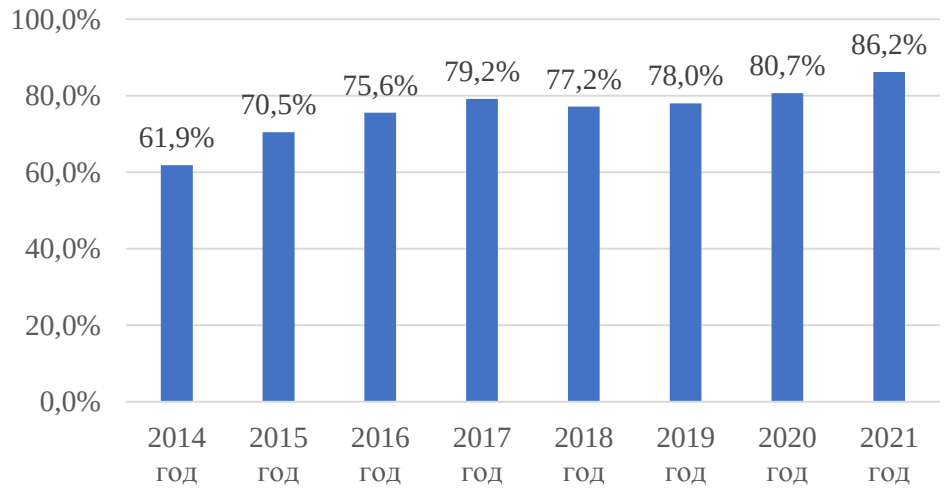

Рисунок 3 – Процент организаций, подвергшихся по крайней мере одной успешной кибератаке

Вопрос о том, как измерить производительность в области кибербезопасности, по-прежнему в значительной степени остается без ответа. Показатели для измерения эффективности кибербезопасности могут быть значительной проблемой в плане измеримости.

Одной из основных целей, преследуемых при обеспечении безопасности киберпространства, является достижение страной способности поддерживать свою экономическую деятельность посредством информационных и коммуникационных технологий (ИКТ). Считается крайне важным, чтобы деятельность, проводимая в киберсреде (банковские операции, сетевые, ритейл, услуги, администрирование и т.д.), была защищена и воспринималась как общая цель для достижения всеми заинтересованными сторонами.

Экономика кибербезопасности применяет принципы экономики к анализу проблем кибербезопасности. Часто считается, что информационная безопасность проявляется только в технических мерах, но экономист Т. Мур охарактеризовал проблему следующим образом: «Люди поняли, что сбой в системе безопасности вызван, по крайней мере, так же часто плохими стимулами, как и плохим дизайном». [10] Это подразумевает, что необходимы

более эффективные стимулы для увеличения инвестиций в кибербезопасность, вместо того, чтобы сосредотачиваться только на технических мерах [11].

В целом работа в этой области включает в себя описания рынка, затрат и выгод, компромиссов рациональных участников рынка, анализ стратегического поведения, рыночные механизмы, сбои и экономические последствия регулирования со стороны правительства.

Великие стратегии прошлого были направлены на «завоевание мира»; парадигма холодной войны превратила это в «сдерживание». Наша эпоха – эпоха окончания эпохальных конфликтов. Мы сохраняем это наследие и хотим достичь «кибермира» с помощью того же мышления, но будущее будет больше зависеть от устойчивости. Частота и интенсивность кибератак являются ярким доказательством того, что истории нет конца. Атомизированный анализ рисков усугубляет системные риски, поскольку сложные системы имеют тенденцию организовываться в направлении катастрофических сдвигов. В этом контексте чрезвычайные меры будет трудно поддерживать, поскольку анализ затрат и выгод обычно проводится постфактум. Инновации снижаются, потому что частный сектор пробует максимизировать эффективность с минимальными инвестициями в инновации.

Экономисты пытаются определить, инвестирует ли рынок социально оптимальный объем в кибербезопасность. Владельцы частных сетей в большинстве случаев не интернализируют свои киберпространства, тогда как в случае осуществления риска убыток затрагивает не только частного владельца сети,но также тысячи других пользователей. Такое явление известно как экстерналия.

IT-отрасль может характеризоваться множеством различных внешних эффектов: внешний сетевой режим, эффекты внешнего отсутствия безопасности и взаимозависимая безопасность. Рассмотрим их немного подробнее:

- внешний сетевой режим. С увеличением объема сети ее ценность для каждого пользователя растет. Примером этого является подъем и доминирование операционной системы Windows;

- отсутствие безопасности порождает негативные внешние эффекты. Отсутствие инвестиций в кибербезопасность одним участником рынка может негативно сказаться на безопасности других. Позитивный экстерналий – это противоположность, когда инвестиции в кибербезопасность одного участника рынка создает повышенный уровень кибербезопасности для всех;

- взаимозависимая безопасность. Такая ситуация происходит, когда один участник рынка, инвестируя в кибербезопасность, создает благоприятные условия безопасности и для других участников, которые, в свою очередь, могут препятствовать собственной безопасности (фридайдинг). Это часто происходит там, где безопасность зависит от самого слабого звена, а участники рынка недостаточно инвестируют в безопасность, так как другие тоже этого не делают. В более широком масштабе, когда страны участвуют в мероприятиях по улучшению своей собственной кибербезопасности, это может повлиять и на других.

Сбой рынка происходит там, где его участники недостаточно инвестируют в безопасность, чтобы соответствовать оказываемым рискам, и именно здесь вмешательство правительства становится решающим [12].

Изучение экономических стимулов дает лучшее понимание рынка, управляемое поведением его участников, и его связи с кибербезопасностью. Их очень мало, и эмпирические данные об имеющихся стимулах свидетельствуют о положительных и отрицательных внешних эффектах. Определенные законодательные стимулы могут простимулировать компании активизировать действия в части выявления угроз и «узких мест» в своих информационных системах. В противном случае организации могут понести потери, в частности такие, как ущерб репутации и доверию, риск ответственности и влияние на финансовые рынки.

Экономический стимул можно охарактеризовать следующим образом: побуждение (мотивация), которое приводит к действию или поведению это предоставление

(положительной) отдачи для участника рынка. Выплаты являются результатом компромисса между затратами и выгодами. Рациональный участник рынка ищет оптимальный выбор, максимизируя отдачу. В экономике полезные функции моделируют компромиссы между затратами и выгодами и, следовательно, представляют собой предпочтения субъектов. В тех случаях, когда результаты выбора являются неопределенными, риск или двусмысленность вводятся в модель принятия решений.

Примеры экономических стимулов были изложены Бауэром и ван Эйтеном (Bauer and van Eeten), в которых они были выделены стимулами, способствующими укреплению безопасности и ее снижению среди участников производственно-сбытовой цепочки ИКТ.

Каждая организация должна решить, сколько она хочет инвестировать в кибербезопасность, и какого уровня кибербезопасности достаточно. Классическая модель рентабельности инвестиций (ROI) — это показатель эффективности, используемый для оценки эффективности инвестиций или сравнения эффективности ряда различных инвестиций. ROI определяется как частное от деления ожидаемой доходности инвестиций на стоимость инвестиций. Однако эта формула не подходит для инвестиций в безопасность, так как безопасность не приносит прибыли; скорее, это предотвращает потери.

Модифицированный расчет ROI может быть применен к инвестициям в безопасность, отсюда и термин «возврат инвестиций в безопасность» (ROSI), который является ключевым показателем эффективности, позволяющим организациям измерять эффективность и результативность расходов на ИТ-безопасность путем сравнения затрат, а также превентивных и корректирующих преимуществ, снижающих вероятность потерь. Это позволяет организации определить, достаточно ли она инвестирует в безопасность, является ли она экономически эффективной и может ли это повлиять на производительность организации, если определенные инвестиции в безопасность не будут сделаны.

Чтобы рассчитать ROSI, необходимо оценить сумму потенциального убытка, который может быть сохранен инвестициями в ценные бумаги, сравнив денежную стоимость инвестиций с уменьшением риска.

Далее рассмотрим количественные оценки риска. Классическим примером для количественной оценки риска является годовая ожидаемая продолжительность убытков (ALE), которая представляет собой общую стоимость инцидента или ожидаемого одного убытка (SLE) (как материального, так и нематериального), умноженного на вероятность риска или годовой коэффициент возникновения (ARO), произошедший в течение этого года.

Модель ROSI сочетает в себе количественную оценку рисков и затраты на внедрение безопасности для конкретного риска. Существуют различные модели ROSI, и нет единой модели, которая подходит всем организациям. При оценке того, какую модель ROSI следует применять, необходимо учитывать несколько факторов, включая степень подверженности риску, характер уязвимостей, тип опасности, отсутствие или слабые места компенсирующих элементов управления, географическое положение, тип и модель бизнеса, критические сектора бизнеса, которые зависят от ИТ, и стратегию конкурентов в отношении ИТ-безопасности.

Формула расчета сочетает в себе ALE (снижение денежных потерь) и предполагаемый процент эффективности определенного решения безопасности со стоимостью инвестиций, чтобы определить, является ли использование определенного решения экономически эффективным [13].

Такие расчеты обычно основаны на собранных метриках внутри организации или из внешних ресурсов. Здесь снова возникают проблемы из-за трудностей оценки потерь, которые могут никогда не возникнуть, и наличия хороших данных, например, об уровне преступности, стоимости ущерба и эффективности контрмер. Оценки часто могут быть предвзятыми из-за нашего восприятия риска, и расчетом можно легко манипулировать, чтобы соответствовать потребностям пользователей для обоснования решения. Поиск точных данных об инцидентах является еще одним препятствием, которое необходимо преодолеть, поскольку многие организации, страдающие от утечек данных, не хотят

делиться этой информацией, часто по репутационным причинам. Кроме того, оценка стоимости может быть проблемой по нескольким причинам:

1) Большая часть информации является засекреченной;

2) Несекретные информационные потоки пропускаются через множество различных организаций для различных видов деятельности;

3) Отсутствуют эффективные механизмы отчетности.

Сложность измерения кибербезопасности проиллюстрирована выше. Большинство из этих моделей и формул используются частным сектором на организационном уровне в различной степени.

Основная дискуссия в доступной литературе сводится к тому, является ли кибербезопасность общественным или частным товаром, и является ли вмешательство правительства необходимым и оправданным для регулирования рынка. Значительные инвестиции уже сделаны частными лицами, предприятиями и в некоторой степени правительствами; однако ясно, что кибербезопасность не может быть оставлена только на усмотрение частного сектора. Это особенно верно для критически важных инфраструктурных секторов страны.

Ситуация позволила некоторым правительствам оправдать вмешательство различными средствами – регулирующими, надзорными, координационными, стимулирующими и дестимулирующими.

В экономической теории товары обычно рассматриваются как государственные или частные. Первый может быть определен как неконкурентный и неисключительный. Неконкурентный товар означает, что использование блага одним человеком не влияет на его использование другими. Неисключительный товар предусматривает, что доступность блага для одного человека означает, что оно также доступно каждому другому человеку. Последнее, частное благо, является товаром, который не может быть использован в неконкурирующей манере.

Кибербезопасность обычно рассматривается как имеющая характеристики частного товара, который продается частными компаниями на рынке правительствам, предприятиям и потребителям. Тем не менее некоторые типы решений кибербезопасности имеют характеристики общественного блага, такие как информация об угрозах и уязвимостях о новых и развивающихся кибервторжениях. Непонимание понятия общественных благ объясняет нежелание делиться информацией, и это часто отражается в законодательных и регуляторных инициативах.

ЗАКЛЮЧЕНИЕ

Исследование основных категорий интернет-вмешательств в деятельность предприятий и анализ возможных угроз экономической безопасности, связанных с киберпространством и использованием сети Интернет, позволили сделать вывод о том, что что компаниям необходимо изменить свое мнение с «если» на них нападут на «когда» и признать, что нарушения конфиденциальности данных или программ-вымогателей могут иметь разрушительные финансовые последствия.

В современных условиях частным предприятиям и банкам следует обратить особое внимание на повышение степени киберзащищенности в связи с резким ростом числа совершаемых преступлений в сети.

Следует отметить, что методы и способы повышения кибербезопасности государства и бизнеса необходимо постоянно совершенствовать. На данный момент острой необходимостью является разработка специального нормативного акта, который можем условно назвать «Стратегия кибербезопасности». Данный документ должен содержать чёткий спектр правовых терминов и определений, касающихся киберохраны государства и других экономических субъектов. А сейчас, вследствие отсутствия определенной правовой базы, правоохранительные органы не имеют должной возможности расследовать количество и категории дел, связанных с информационным пространством и интернет-технологиями. В

стратегии должны быть также указаны основные риски и угрозы кибербезопасности, цели, принципы, приоритеты и направления деятельности государства по обеспечению безопасности в киберпространстве.

Федеральное руководство, в свою очередь, обязано быть готовым к кризисным ситуациям и финансированию сервисов кибербезопасности, а также принимать адекватные и незамедлительные меры, направленные на пресечение киберугроз и распространение дезинформации.

СПИСОК ЛИТЕРАТУРЫ

1) Аудитория интернета в России в 2020 году [Электронный ресурс]. Режим доступа: https://mediascope.net/news/1250827/ (дата обращения: 15.01.2022)

2) Горбунова, В. Б. Методические аспекты управленческой деятельности в современных экономических условиях / В. Б. Горбунова // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2015. – № 3(41). – С. 127–130.

3) Безопасность превыше всего: об экономических рисках и будущих угрозах развития цифровых технологий / Е. К. Карпунина, С. С. Моисеев, Е. В. Лисова, А. Ф. Бейлина // Вестник Северо-Кавказского федерального университета. – 2019. – № 6(75). – С. 86–94. – DOI 10.37493/2307-907X-2019-75-6-86-94.

4) Bolshenko, S. F. A methodological approach to determining the competitive positions of the labor potential in regional consumer cooperation / S. F. Bolshenko, V. B. Gorbunova, O. V. Martynenko // Studies in Systems, Decision and Control. – 2021. – Vol. 316. – P. 661-670. – DOI 10.1007/978-3-030-57831-2_71.

5) Проблемы безопасности в электронном бизнесе [Электронный ресурс]. Режим доступа: http://iso.ru/ru/press-center/journal/1765.phtml (дата обращения: 22.01.2022)

6) Торшхоев, С. М. А. Кибермошенничество как угроза экономической безопасности в контексте пандемии SARS COV-2 / С. М. А. Торшхоев, Ф. К. Иванов // Актуальные исследования. – 2021. – № 19(46). – С. 51-54.

7) Оценка рисков и классификация угроз экономической безопасности на рынке электронной торговли [Электронный ресурс].Режим доступа: https://studme.org/331416/ekonomika/otsenka_riskov_klassifikatsiya_ugroz_ekonomicheskoy_bezopasnosti_rynke_elektronnoy_torgovli (дата обращения: 5.05.2021)

8) Cybersecurity Statistics and Trends for 2021 [Электронный ресурс]. Режим доступа: https://purplesec.us/resources/cyber-security-statistics/ (дата обращения: 15.01.2022)

9) Report Defense Cyberthreat 2021 [Электронный ресурс]. Режим доступа: https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf (дата обращения: 25.01.2022)

10) Introducing the Economics of Cybersecurity: Principles and Policy Options [Электронный ресурс]. Режим доступа: http://static.cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf (дата обращения: 17.02.2022)

11) Горбунова, В. Б. Современные тенденции развития научнотехнической безопасности территорий / В. Б. Горбунова // Балтийский экономический журнал. – 2020. – № 2(30). – С. 39–45.

12) Гальчевская, А. Р. Исследование потенциальных источников дестабилизации экономической безопасности Калининградского региона / А. Р. Гальчевская, В. Б. Горбунова // Вестник молодежной науки. – 2019. – № 3(20). – С. 3.

13) Economic aspects of national cyber security strategies - Pascal Brangetto, Mari Kert-Saint Aubyn 2015 [Электронный ресурс]. Режим доступа: https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf (дата обращения: 20.01.2022)

CURRENT SECURITY THREATS ECONOMIC SECURITY IN CYBERSPACE

L.V. Chernykh, 3rd year student
e-mail: vafleman@gmail.com
Kaliningrad State Technical University

V.B. Gorbunova, PhD, Associate Professor
e-mail: viktoriya.gorbunova@klgtu.ru
Kaliningrad State Technical University,

The article explores the current threats to economic security in cyberspace. As the pandemic spread, society and the state faced another global problem in the face of a series of cyber attacks and cyber crimes by computer scammers, while in proportion to the growth in the number of cyber crimes, the damage they cause is growing. The paper outlines an approach to calculating the effectiveness of measures to increase the level of cybersecurity. Based on the results of the analysis, the main directions are identified, possible methods and ways to improve cybersecurity in modern conditions. It was found that only through the joint efforts of the state and business it is possible to neutralize the threats to economic security in the context of the expansion of cyberspace, which is inevitably accompanied by the identification of more and more new types of cyber attacks, fraud and other information crimes.

Key words: cybersecurity, cybercrime, fraud, cyber fraud, economic security, risks, threats, information technology.