ECONOMICS

Kirilchuk S.P., Nalivaychenko E.V.

THE APPROACHES TO THE PROBLEM SOLVING OF PROTECTION OF INTERNATIONAL COMPANIES' INFORMATION

Kirilchuk S.P., Russia, V.I. Vernadsky Crimean Federal University, doctor of economics, professor
Nalivaychenko E.V., Russia, V.I. Vernadsky Crimean Federal University, doctor of economics, professor

Abstract
The article examines the problems of the development of the information society in the context of globalization: the Internet, intellectual property information systems. Considered possible approaches to ensuring the safety of the automated information system of an international company: fragmented and complex.
Keywords: automated information system; protection of information; cybercrime; antivirus software; a fragmented approach to the protection of information; a comprehensive approach to information protection.

Введение. В последнее время приобрели глобальный масштаб проблемы, связанные с интеллектуальным (компьютерным, информационным) пиратством. Есть общие причины и последствия пиратства в софтверном мире. В решении проблемы безопасности информационной системы международных компаний сложились два подхода, которые можно условно назвать фрагментарным и комплексным.

Материалы и методы исследования (эксперимент). Под системой защиты информационной системы будем понимать единую совокупность правовых и морально-этических норм, организационных, технологических и программно-технических мероприятий и программно-

технических средств, направленных на противодействие угрозам информационной системе с целью сведения к минимуму возможного ущерба пользователям и владельцам систем.

Организуя защиту информационной системы, желательно определить возможность осуществления каждого конкретного вида угрозы и размер потенциального ущерба, который испытывают пользователи и владельцы информационной системы, если угроза реализуется. Для этого исследуем фрагментарный и комплексный подходы к защите информации международной компании.

Результаты и обсуждение. Любой подход к организации работы информационной системы меры по ее безопасности вызывают определённые проблемы. Главные из них, на наш взгляд: дополнительное усложнение работы с большинством защищенных систем; увеличение стоимости защищенной системы; дополнительная нагрузка на системные ресурсы, что требует увеличения рабочего времени для выполнения того же задачи в связи с замедлением доступа к данным и выполнением операций в целом; необходимость привлечения дополнительного персонала, ответственного за поддержание работоспособности системы защиты.

Охарактеризуем наиболее типичные ситуации, в которых создается угроза безопасности информационных систем, используя соответствующие положения Окинавской Хартии глобального информационного общества, принятую 22 июля 2000 года лидерами стран «Большой Восьмёрки» [1].

Несанкционированный доступ – один из самых распространенных видов компьютерных нарушений, который заключается в получении пользователем доступа к объекту, на который у него нет разрешения согласно принятой в данной системе политикой безопасности.

Несанкционированный доступ становится возможным из-за неудачного выбора средств защиты, их некорректной установки и настройки, а также из-за небрежного отношения к защите собственных данных.

Незаконное использование привилегий. В любой защищенной системе предусмотрены средства, которые используют при чрезвычайных ситуациях, или средства, которые способны функционировать даже в случае нарушения правил введенной политики безопасности. Например, в случае неожиданной проверки работы системы пользователь должен иметь доступ ко всем наборам системы. Конечно, эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющих специальные функции.

Под угрозой безопасности понимается потенциально возможное влияние, которое может прямо или опосредованно нанести вред пользователям или владельцам информационных систем [2, 3, 4].

Подвергаться опасности могут [5, 6]:

– информационная система в целом – злоумышленник пытается проникнуть в систему для дальнейшего выполнения каких-либо несанкционированных действий. Для этого он обычно использует метод «маскарада», перехват или подделки пароля, взлома;

– объекты информационной системы – данные или программы в оперативном запоминающем устройстве (ОЗУ) или на внешних носителях; сами устройства системы как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (ОЗУ, процессор). Преступное влияние на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности информации, на них сохраняется), или нарушение их функциональности (например, заполнение всей ОЗУ бессмысленной информацией или загрузки процессора компьютера задачей с неограниченным временем выполнения);

– субъекты автоматизированной системы, то есть процессы или подпроцессы пользователей. Целью таких атак является прямое влияние на ход процесса - его прекращение, изменение привилегий, или обратное влияние - использование злоумышленником привилегий и характеристик иного процесса;

– каналы передачи данных (сами каналы или пакеты данных, передаваемых по каналу). Влияние на пакеты данных может рассматриваться как атака на объекты сети; влияние на каналы - как специфический тип атак, характерный для определенной сети.

От состояния объекта атаки в момент ее совершения во многом зависят результаты атаки и меры по ликвидации ее последствий. Объект атаки может находиться в одном из двух состояний:

- хранения информации на машинном носителе в пассивном состоянии. При этом воздействие на объект осуществляется с использованием доступа передачи информации по линии связи между узлами сети или внутри узла. Влияние предполагает доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), или просто прослушивание с использованием тайных каналов;
- обработки информации в тех ситуациях, когда объектом атаки является процесс пользователя.

Классифицируют угрозы безопасности информации и по другим признакам: по цели реализации, по принципу действия, по характеру воздействия и тому подобное. Численность классификаций

предопределяет сложность как определения опасности, так и средств защиты от нее.

В Будапеште 23 ноября 2001 года Советом Европы была открыта для подписания Конвенция о компьютерных преступлениях [7]. Все киберпреступления классифицируются по следующим типам:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.

2. Правонарушения, связанные с использованием компьютерных средств.

3. Правонарушения, связанные с содержанием данных (например, детская порнография).

4. Правонарушения, связанные с нарушением авторского права и смежных прав.

5. Покушение, соучастие или подстрекательство к совершению преступлений, описанных в пунктах 1-4.

Однако Конвенция не подписана Российской Федерацией. По мнению экспертов, ряд положений Конвенции противоречит некоторым нормам российского законодательства. В частности, некоторые статьи предусматривают предоставление трансграничного доступа к компьютерным данным, что может нанести ущерб информационной безопасности государства.

Одной из самых больших угроз информационных систем является поражение вирусными программами, проникающими через различные носители информации, особенно через глобальные информационные сети. По мнению Владимира Тихонова, специалиста службы консалтинга «Лаборатории Касперского», в 2016 году было зафиксировано 7 крупных вирусных эпидемий. Эпидемии 2016 года он делит на следующие группы: вирус Nyxem.e, вирусы семейств Bagle и Warezov, среди которых много почтовых червей, а также вариант троянца-шифровальщика Gpcode. В 2016 году появилось около 60 тыс. новых вирусов, что на 41% больше, чем в 2015 году [8].

Распространению этих программ способствует то, что большинство программистов-создателей вирусных программ, ничего на имеют против открытости кода их программ. Эти программы свободно появляются в печатных изданиях. На самом деле закрытой является уязвимость программ. Так, уязвимость в процедуре обработки WMF-файлов в конце прошлого года продавалась за 4 тысячи долларов [8].

Если рассмотреть зарубежный опыт, то, например, компания Cisco Systems, которая насчитывает около 57 000 сотрудников, рассредоточенных по всему миру, продолжает традиции новаторства и разрабатывают лучшие в отрасли продукты и решения в сфере современных технологий, к которым относятся: IP-коммуникации; сетевая безопасность; беспроводные сети LAN; домашние сети; видеосистемы;

прикладные сетевые услуги. К важнейшим проблемам безопасности руководство компании относит проблемы проникновений вирусов, разворовывание информации, снижение эффективности работы компьютеров в связи с использованием их ресурсов злоумышленниками для других целей, большую скорость модификации угроз, несовершенство законодательной базы [9].

Пиратство программного обеспечения (ПО) как таковое имеет три основных направления негативного воздействия:

- Экономическое – пиратство наносит экономический ущерб не только из-за ухудшения инвестиционного климата, но также из-за недополучения налогов при продаже легального софта, потому что пираты налогов не платят.

- Интеллектуальное – пиратство способствует уничтожению индустрии ПО. Кроме того, авторские права на программное обеспечение – экономической основы софтверной индустрии - российским программистам оформлять затруднительно ввиду, опять же, несовершенства международной законодательной базы.

- Технологическое – пиратские версии ПО имеют низкое качество и это влияет как на возможность их качественного использования, так и на формирование негативного имиджа компании-производителя лицензированного продукта.

- Политическое – развитое пиратство ухудшает имидж и инвестиционный климат государства. Россия относится к «Перечню стран приоритетного наблюдения» (Priority Watch List) (табл. 1) в рамках списка «Special 301» [10]**.** Согласно исследованию международной консалтинговой компании «Yankee Group», а также организации «Business Software Alliance» 35% всего ПО в мире является нелицензионным. Из 97 стран, где проходило исследование, в 51-й уровень пиратства составляет не менее 64% [11].

Рассмотрим два подхода, которые сложились в решении проблемы безопасности информационной системы международных компаний, и которые можно условно назвать фрагментарным и комплексным.

Фрагментарный подход, ориентированный на противодействие строго определенным угрозам при определенных условиях, предполагает применение, например, специализированных и автономных средств шифрования и тому подобное. Шифрованием занимается много известных международных компаний, среди которых выделяются Cisco и RSA, услугами которых пользуются многие пользователи мира и которые объединили усилия для производства новой технологии в области информационной безопасности, с помощью которой будет происходить управление процессом шифрования на разных устройствах хранения информации: дисках, ленточных накопителях и виртуальных библиотеках.

Эта технология может успешно работать в сетевом режиме [12]. Главное преимущество фрагментарного подхода заключается в его высокой вариативности защиты против конкретной угрозы. Но ему присущ и такой недостаток, как локальность действия, то есть фрагментарные методы обеспечивают эффективную защиту конкретных объектов информационной системы от конкретной угрозы, но не более того. Даже небольшая модификация угрозы приводит к потере эффективности защиты.

Таблица 1 - Список стран приоритетного наблюдения (Priority Watch List) в рамках списка IIPA 2014 «Special 301» (ориентировочные потери в результате нарушения прав интеллектуальной собственности за 2014 год)

Страна	Деловое ПО		Общий ущерб от пиратской деятельности, млн. долл. США
	млн. долл. США	уровень пиратства	
Аргентина	215,0	76%	301,0
Венесуэла	124,0	84%	174,6
Доминиканская республика	10,0	77%	20,9
Египет	47,0	63%	90,0
Израиль	41,0	32%	98,4
Индия	318,0	70%	496,3
Канада	551,0	34%	551,0
Китай	1949,0	82%	2207,0
Коста-Рика	12,0	65%	27,1
Мексика	296,0	63%	1005,6
Россия	1433,0	83%	2180,1
Саудовская Аравия	112,0	51%	140,0
Таиланд	164,0	80%	219,7
Турция	203,0	66%	243,0
Украина	290,0	85%	320,0
Чили	65,0	64%	95,6

При комплексном подходе сочетаются разнородные меры противодействия угрозам (правовые, организационные, программно-технические и т. д.) В целом в комплексе все эти меры формируют политику безопасности экономической информации.

Комплексный подход эффективен для защиты крупных информационных систем, нарушение безопасности которых может нанести огромный материальный ущерб. Но комплексный подход пригоден и для небольших информационных систем, обрабатывающих особо ценную информацию или выполняющих ответственные задачи.

Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий, и учреждений. Он находит отражение в различных стандартах. Недостатками комплексного подхода является сложность управления и ограничения на свободу действий пользователей информационной системы. Ярким примером комплексного подхода к защите информационной системы является семейство продуктов для обеспечения безопасности бизнеса Microsoft Forefront для сетевой структуры, созданный международной компанией Microsoft. Одним из преимуществ этого семейства является интеграция средств обеспечения безопасности с серверными приложениями Microsoft и существующей инфраструктурой [10].

Построение любой системы защиты международной компании, на наш взгляд, предусматривает ряд этапов, подобных этапам создания самих информационных систем. В частности, к ним относятся:

- анализ возможных угроз информационной системе;
- разработка системы защиты;
- реализация системы защиты;
- сопровождение системы защиты.

Управлять электронными ресурсами международной компании нельзя без мер безопасности [13].

Административные меры защиты — это меры организационного характера, регламентирующие процессы функционирования информационной системы, использование ее ресурсов, деятельность персонала и т. д. Цель этих мероприятий - в наибольшей степени исключить возможность реализации угроз безопасности. В перечень административных мер можно отнести следующие:

- разработка правил обработки информации в информационной системе;
- организация защиты от установки аппаратуры прослушивания в помещениях вычислительного центра;
- тщательный отбор персонала;

- организация учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;
- распределение реквизитов разграничения доступа (паролей, профилей полномочий и т. д.);
- организация скрытого контроля за работой пользователей и персонала информационной системы;
- другие мероприятия.

Физические меры защиты – это разного рода механические, электро- или электронно-механические устройства и строения, предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам защиты информации.

Технические (аппаратно-программные) средства защиты – различные электронные и специальные программы, выполняющие функции защиты. Среди таких функций отметим следующие: идентификация и аутентификация (соответствие требованиям на верность) пользователей или процессов, разграничения и контроля доступа к ресурсам, регистрация и анализ событий, криптографическая защита информации (шифрование данных), резервирование ресурсов и компонентов информационной системы.

К аппаратно-программным мероприятиям относятся антивирусные программы. Большую популярность на рынке программных продуктов завоевали антивирусные программы лаборатории Касперского. Эти программы используются для борьбы с различными видами вирусов. Так, в связи с возникновением новой угрозы поражения мобильных телефонов эта лаборатория и компания PlayMobile (холдинг Next Media Group) запустили на российском рынке новый сервис – антивирусная защита мобильных телефонов. Высокоэффективным средством борьбы с вредоносными программами на ПК, ноутбуках, серверах является недавно выпущена обновленная версия Symantec Endpoint Protection антивирусного продукта Symantec [14], которая изготавливается одноименной международной компанией. Кроме защиты от вирусов эта программа обеспечивает защиту от шпионского ПО, межсетевой экран, систему предотвращения вторжения, охрану от вредоносных объектов удаленных рабочих мест. Лучшими антивирусными продуктами 2016 года считаются Avira, Bitdefender, российское решение Лаборатории Касперского [15]. Они осуществляют сбалансированную защиту от угроз персонального компьютера от вирусов, червей, троянских, шпионских и других вредоносных программ. Также обеспечивают защиту корпоративных сетей, централизованное обновление, инструменты удаленного администрирования и управления защитой всей сети с одного рабочего места. Наилучшие результаты достигаются при системном подходе к

проблемам безопасности информационной системы и комплексного применения мер защиты на всех этапах жизненного цикла системы, начиная с ранних стадий ее проектирования. Однако там, где это возможно, другие меры надо заменить более надежными современными физическими и техническими средствами.

Экономическая политика безопасности складывается из следующих составляющих. В процессе анализа риска изучают компоненты информационной системы, могут испытать посягательств на их безопасность, определяют уязвимые места системы, оценивают возможность реализации для каждой конкретной угрозы и ожидаемые размеры соответствующих потерь, выбирают возможные методы защиты и вычисляют их стоимость. На заключительном этапе оценивается выгода от применения предлагаемых мер защиты. Эта выгода может иметь как положительный, так и отрицательный знак: в первом случае – речь идет об очевидном выигрыше, а во втором – о дополнительных расходах для обеспечения собственной безопасности.

Исходя из результатов этого анализа, принимают решение о целесообразности тех или иных мер защиты. В конечном итоге составляется план защиты, формируется экономическая политика безопасности.

На наш взгляд, эффективный план защиты должен содержать следующие разделы:

- текущее состояние системы;
- рекомендации по реализации системы защиты;
- ответственность персонала;
- порядок введения средств защиты;
- порядок пересмотра плана средств защиты и их состав.

Экономическая политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, которые реализуются с помощью организационных мер и программно-технических средств, и определяющей архитектуры системы защиты. Для конкретных международных компаний политика безопасности должна быть индивидуальной. Она зависит от конкретной технологии обработки информации, используемых программных и технических средств, расположения организации и т. д.

Роль сетевой информации в развитии современных международных компаний растет. Одной из главных проблем процесса информатизации является хакерские атаки на информационные системы, которые наносят прямые материальные убытки не только разработчикам информационных технологий, но и их пользователям. Symantec выпустила комплексный отчет о безопасности, составляемый аналитиками компании каждые полгода [14]. Главный вывод, содержащийся в документе, состоит

в том, что в США по-прежнему создается больше всего вредоносных программ. Именно на территории США действует максимальное количество хакерских группировок, которые делают больше атак, чем в любой другой стране мира.

Также в Symantec отмечают, что между хакерскими группировками существует довольно жесткая конкуренция на подпольном рынке взломов и торговли краденой информацией. Именно благодаря данной конкуренции, по словам экспертов, купить сегодня ворованные данные можно дешевле и проще, чем еще полгода назад.

В отчете Internet Security Threat Report Symantec приводит ряд примеров: например, в начале текущего года специалисты компании смогли приобрести краденые номера пластиковых банковских карт по цене $ 1 за каждый номер, а также на черном рынке в США присутствуют и различные банковские базы данных. Однако в отличие от России, где такая информация стоит от $ 70 до $ 1000 за CD, в США средняя стоимость диска с ворованными банковскими данными (счета, проводки и т.д.) стоит всего $ 14, утверждают в Symantec.

Также отмечается, что около 30% от общего количества компьютерных атак в второй половине 2016 г. было осуществлено американскими злоумышленниками.

По количеству генерирующего злонамеренного кода США также занимают первое место в мире - за отчетный период в США была создана каждая третья шпионская программа и написан каждый третий вирус троян. На втором месте – Китай с 10%, третье место за Германией – 7%.

Кроме этого, США лидируют и по количеству ботов-сетей, состоящих из инфицированных компьютеров, с помощью которых хакеры рассылают спам и делают атаки. В подавляющем большинстве случаев владельцы компьютера не догадываются о том, что машина инфицирована и тратят процессорное время и трафик в интересах хакеров.

Symantec также отмечает и рост спама во второй половине 2016 года на 59%, что, как говорят специалисты, довольно много, если учесть 5%-ный рост спама в первом полугодии 2016 года. Более всего спама в международном масштабе было связано с игрой на бирже и различных финансовых махинациях.

Одной из самых мощных компаний, распространяющих антиспамные программы, является компания McAfee. Кроме этого, она разрабатывает программное обеспечение, ведет борьбу против фишинга, червей, вирусов. Опциональный модуль защиты от спама обнаруживает и блокирует спам и фишинг, а защита всегда осуществляется в соответствии с текущими обновлениями.

Впервые в Symantec изучили активность на международном электронном рынке сетевых мошенников (фишеров), создающих сайты, имитирующие сайты крупных магазинов или банков с целью краж

персональных данных посетителей. По словам Альфреда Хьюгера, вице-президента подразделения Symantec Security Response, фишинг стал в высшей степени организованным, высокоразвитым и без каких-либо моральных барьеров. Рост количества сайтов-подделок составил 65% по сравнению с первым полугодием 2016 года.

По данным отчета международной компании Aladdin Malware Report 2016, если в 2015 году 60% данных, полученных с помощью программ-шпионов и троянцев, относились к незначительным угрозам, то в 2016 году большая часть троянских и шпионских приложений имели статус среднего и критического уровня. Исходя из данных отчета Aladdin:

– 65% шпионских приложений можно отнести к классу троянских;

– 30% шпионских приложений ведут рассылку спама;

– 15% шпионских приложений одновременно ведут учет данных, вводимых пользователем с клавиатуры;

– 10% шпионских приложений используют механизмы, характерные для руткитов (программ, работающих на уровне ОС и служат для защиты и обнаружения).

По мнению более 90% IT-специалистов, в 2017 году главной угрозой корпоративной информационной безопасности станут устройства «Интернета вещей» (IoT). Однако действующие в компаниях программы по обеспечению безопасности не поспевают за новыми угрозами. К таким выводам пришли эксперты Pwnie Express на основании опроса IT-специалистов [16].

Также борьба в международных информационных сетях ведется и против вирусов, которые могут проникать к компьютерам по сети. Средствами борьбы является как антивирусные программы, упомянутые ранее, так аппаратно-программные средства. Одним из них является полученное в результате партнерства между компаниями Sophos и SurfControl программно-аппаратное решение WS1000, которое обеспечивает безопасность в Интернете. В это устройство интегрировано приложение для систематизации URL-адрес, который имеет данные о более чем 21 млн Web-страниц. Это решение позволяет администраторам управлять производительностью конечных пользователей с помощью систематизированной базы данных Web-сайтов. Также существующие технологии Sophos обеспечат защиту от известных и неизвестных вирусов, червей, троянских программ, рекламного шпионского программного обеспечения, а также фишинговых Web-сайтов.

Наличие национальных границ, пересекающих линию связи, усложняет ситуацию относительно прав собственности в информационных сетях, ведь авторские и патентные права в разных странах разные. Например, в сети можно найти интересный том забытой технической документации, авторские права на которую в данной стране

уже не действительны за давностью. Пересылка таких файлов в эту страну может поставить пользователей вне федеральных законов той страны, откуда ссылаются файлы. Следует убедиться, есть ли на это разрешение. Проблема еще и в том, что законодательство об электронных коммуникациях не успевает за прогрессом технологии. Даже если есть разрешение передачи по e-mail, это еще не значит, что послание, переданное по электронной почте, имеет какую-нибудь реальную защиту.

Открытое обсуждение проблем безопасности информации, возникающей в международных информационных системах, является частью самой проблемы безопасности [13]. Необходимо обсуждать и исследовать эти проблемы, находить решения и информировать достойных доверия специалистов. В США для этих целей правительством основана организация CERT: Computer Emergency Response Team (группа реагирования на компьютерную опасность). CERT исследует проблемы безопасности, работает с производителями над их решением, объявляет о принятых решениях, создает много служб помощи, в которых пользователи могут узнать о защищенности собственных компьютеров. Отделение CERT предпочитают работать непосредственно с местными силами безопасности, но не откажутся ответить на вопрос каждого в случае опасности.

Выводы. Известно, что инновации дают 80% экономического роста. Учитывая текущую ситуацию в мировой экономике, особенно рост неравенства в развитых странах и дисфункцию потребительских экономических моделей во многих развивающихся государствах, неудивительно, что экономические прорывы ближайшего будущего связаны с инновациями в таких областях, как информатизация, биотехнологии, генная инженерия, 3D-печать, робототехника, автоматические системы управления.

К важнейшим проблемам безопасности международных компаний относят проблемы проникновений вирусов, разворовывание информации, снижение эффективности работы компьютеров в связи с использованием их ресурсов злоумышленниками для других целей, большую скорость модификации угроз, несовершенство законодательной базы.

Наличие национальных границ, пересекающих линию связи, усложняет ситуацию относительно прав собственности в информационных сетях, поскольку авторские и патентные права в разных странах разные, и единое законодательное поле для функционирования международных компаний не создано.

Исследование показало, что причинами выхода из строя машин в международной информационной сети является наличие следующих угроз:

– установление доступного пароля;

– импорт легальными пользователями испорченного программного обеспечения;
– нехватка системного обеспечения;
– несоблюдение режима защиты от вирусов.

Компьютеры, работающие в операционных системах со многими задачами, которые выполняют задачи для международных компаний, (типа Unix, VMS), более открыты для заражения вирусами, поэтому их следует особенно тщательно защищать от несанкционированного доступа. Экономическая политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, которые реализуются с помощью организационных мер и программно-технических средств, и определяющей архитектуры системы защиты. Для конкретных международных компаний политика безопасности должна быть индивидуальной. Она зависит от конкретной технологии обработки информации, используемых программных и технических средств, расположения организации и т. д.

В решении проблемы экономической безопасности информационной системы международной компании сложились два подхода, которые можно условно назвать фрагментарным и комплексным.

Главное преимущество фрагментарного подхода заключается в его высокой вариативности защиты против конкретной угрозы. Но ему присущ и такой недостаток, как локальность действия, то есть фрагментарные методы обеспечивают эффективную защиту конкретных объектов информационной системы от конкретной угрозы, но не более того. Даже небольшая модификация угрозы приводит к потере эффективности защиты.

Комплексный подход эффективен для защиты крупных информационных систем, нарушение безопасности которых может нанести огромный материальный ущерб, а также применим и для небольших информационных систем, обрабатывающих особо ценную информацию или выполняющих ответственные задачи. Недостатками комплексного подхода является сложность управления и ограничения на свободу действий пользователей информационной системы. При комплексном подходе сочетаются разнородные меры противодействия угрозам (правовые, организационные, программно-технические и т.д.). В целом в комплексе все эти меры формируют политику безопасности экономической информации. Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий, и учреждений в мире. Он находит отражение в различных стандартах.

Построение любой системы экономической информационной защиты международной компании, должно предусматривать ряд этапов: анализ возможных угроз информационной системе; разработка системы защиты; реализация системы защиты; сопровождение системы защиты.

Открытое обсуждение проблем безопасности информации, возникающей в международных информационных системах, является частью самой проблемы безопасности. Необходимо обсуждать и исследовать эти проблемы, находить решения и информировать достойных доверия специалистов.

References:

[1] Okinawa Charter on Global Information Society (Okinawa, 22 July 2000). N.p., n.d. Web. 17 Apr. 2017. <http://en.unesco.org/>.
[2] The Information Security Doctrine of the Russian Federation (App. by the Decree of the President of the Russian Federation of December 5, 2016 N 646). Legal Information Portal GARANT.RU. N.p., n.d. Web. 12 Apr. 2017. <http://ivo.garant.ru/#/document/71556224/paragraph/9:3>.
[3] Strategy of Information Society Development in Russia (App. By the President of the Russian Federation on 7 February 2008 № PR-212). Legal Information Portal GARANT.RU. N.p., n.d. Web. 12 Apr. 2017. <http://www.garant.ru/products/ipo/prime/doc/92762/#ixzz4eiU25bCS>.
[4] Federal Law of the RF "About Information, Information Technologies and Protection of Information" of 27.07.2006 № 149-FZ. Legal Information Portal GARANT.RU. N.p., n.d. Web. 12 Apr. 2017. <http://ivo.garant.ru/#/document/12148555/paragraph/3471:7>.
[5] Cleary, Liam. "The Tendencies of Development of Information Technologies." Windows ITPro/re. №4 Apr. 2017: 18-20. Print.
[6] Computer World №2. Feb. 2014. Magazines online. Web. 10 Apr. 2017. <http://jurnali-online.ru/kompyuternie/kompyuternyj-mir-2-fevral-2014.html>.
[7] The Convention on Cybercrimes (Budapest, 23 November 2001). N.p., n.d. Web. 17 Apr. 2017. <http://worldlaws.narod.ru/konvenc/00009.htm>.
[8] Information-analytical Resource "Your Personal Internet". N.p., n.d. Web. 17 Apr. 2017. <http://www.content-filtering.ru/catalog.asp?ob_no=1660>.
[9] Gartner, Inc. N.p., n.d. Web. 7 Apr. 2017. <http://www.dataquest.com/press_gartner/quickstats/ITSpending.tml>.
[10] Panasenko, A. "Overview of Forefront Client Security from Microsoft." N.p., n.d. Web. 17 Apr. 2017. <https://www.anti-malware.ru/node/57>.
[11] International Intellectual Property Alliance. N.p., n.d. Web. 10 Apr. 2017. <http://www.securitylab.ru/news/291275.php>.
[12] "New Intel 2017." 2017god.com. N.p., n.d. Web. 12 Apr. 2017. <http://2017god.com/novye-processory-intel-2017-goda/>.

[13] Nalivaychenko E.V. Improvement of the Intellectual Assets Management in the Information Economy/ Nalivaychenko E.V. Kirilchuk S.P //Journal of Applied Economic Sciences (Romania) Summer 2016 Volume XI, Issue 4(42), c. 662-671 (Scopus).
[14] Symantec Antivirus Product. N.p., n.d. Web. 10 Apr. 2017. <http://www.symantec.com/endpointsecurity>.
[15] "Experts Have Called the Best Antivirus 2016." Planet-today.ru – News Portal. N.p., 10 Feb. 2017. Web. 15 Apr. 2017. <http://planet-today.ru/novosti/tekhnologii/item/63275-eksperty-nazvali-luchshij-antivirus-2016-goda.>.
[16] Levenkov, O. "90% of Information Security Experts Consider IoT a Major Security Threat in 2017." The Company "Aladdin R. D.", n.d. Web. 17 Apr. 2017. <https://www.aladdin-rd.ru/company/pressroom/articles/45240/>.

Evlakhova Yu.S., Brichka E.I.

COUNTERACTION TO MONEY «CASHING IN»: CHARACTERISTICS OF THE PROBLEM AND ANALYSIS OF MECHANISMS OF ITS SUPPRESSION IN RUSSIAN BANKS

Evlakhova Yu. S., Russian Federation, candidate of economics, associate professor of the Department "Financial monitoring and the financial markets", Rostov State University of Economics (RINH)

Brichka E. I., Russian Federation, candidate of economics, associate professor of the Department "Financial monitoring and the financial markets", Rostov State University of Economics (RINH)

Abstract

Article is devoted to a research of counteraction mechanisms to illegal money "cashing in" on the basis of the analysis of the Russian practice of fight against shadow "cashing" platforms during the period from 2010 to 2016. It is revealed that despite distinctions of scientific approaches to the concept "cashing in", the negative impact of this process on a financial system and national economy in general is recognized as both the regulator, and experts. In work the main schemes on money "cashing in" by natural persons, individual entrepreneurs and legal entities, widespread in the Russian banks are selected. The mechanisms of counteraction to money "cashing in" used in the Russian banks are opened and need of use of economic losses from illegal "cashing in" calculation method for increase in efficiency is proved.

Keywords: "cashing in", money laundering, illegal bank activity, shadow economy, counteraction to money laundering

Проблема незаконного «обналичивания» денежных средств продолжает сохранять свою актуальность для российской экономики. Согласно данным Счетной палаты Российской Федерации, в 2006 г. рынок «обналиченных» денежных средств в РФ был сопоставим с федеральным бюджетом [1]. В современных реалиях этот показатель не достигает таких масштабов, однако остается весьма существенным: в 2017 году в РФ