МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Белорусский национальный технический университет

Кафедра «Таможенное дело»

Г. М. Бровка
И. А. Ковалькова
А. Н. Шавель

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТАМОЖЕННЫХ ОРГАНАХ

Учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело»

Рекомендовано учебно-методическим объединением по гуманитарному образованию

Минск
БНТУ
2019

УДК 339.543:004.056.5(075.8)
ББК 65.428я7
Б88

Р е ц е н з е н т ы:
кафедра «Таможенное дело» УО «Белорусский государственный университет транспорта» (зав. кафедрой – канд. экон. наук, доцент *О. В. Морозова*);
декан факультета «Информационные технологии и робототехника» БНТУ, канд. физ.-мат. наук, доцент *Е. Е. Трофименко*;
доцент кафедры «Вычислительная математика» БГУ, канд. физ.-мат. наук, доцент *А. М. Будник*

Бровка, Г. М.

Б88 Информационная безопасность в таможенных органах : учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. – Минск: БНТУ, 2019. – 118 с.

ISBN 978-985-583-260-8.

В учебно-методическом пособии рассмотрены основные понятия, проблемы и угрозы информационной безопасности, наиболее важные направления ее обеспечения. Обсуждаются вопросы правового и организационного обеспечения информационной безопасности, информационного обеспечения деятельности таможенных органов Республики Беларусь.

Предназначено для студентов, обучающихся по специальности таможенного дела, менеджмента, слушателей ГИПКиПКТО, специалистов, должностных лиц таможенных органов, преподавателей.

УДК 339.543:004.056.5(075.8)
ББК 65.428я7

ISBN 978-985-583-260-8

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Мир и безопасность по праву занимают ведущее положение в системе основополагающих человеческих ценностей. Несмотря на существование массы международных организаций, включая Организацию Объединенных Наций (далее – ООН), а также союзов и блоков, конкретного практического воплощения общих и универсальных подходов к безопасному существованию на планете пока не произошло. Главный системный недостаток заключается в отсутствии глобальных гарантий соблюдения принципа неделимости безопасности.

Актуальность данной темы состоит в том, что каждое государство, исходя из интересов своего народа, вынуждено опираться в вопросах обеспечения безопасности в первую очередь на собственные возможности. Причина проста – безопасность выступает непременным и необходимым условием самого существования страны, общества, нации.

Еще на этапе становления независимого белорусского государства был избран фундаментальный подход – обеспечение национальной безопасности Республики Беларусь как безопасности личности, общества и государства. Впервые он нашел отражение в Концепции национальной безопасности, утвержденной в 1995 году. В 2001 году, исходя из развития внутриполитической и международной обстановки, ряд положений Концепции был скорректирован. К 2010 году ряд угроз, естественно, утратил былую актуальность. Однако новое звучание получили экологические и другие общечеловеческие проблемы.

Обострились проблемы безопасности в политической сфере. Прежде всего, это выражалось в использовании отдельными странами или коалициями новых стратегий и методов, затрудняющих обеспечение другими государствами своих законных национальных интересов в данной области. На этом фоне подходы к национальной безопасности объективно не могли пребывать в застывшем состоянии. Поэтому Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 была утверждена Концепция, которая действует и в настоящее время.

В документе сохранена преемственность с ранее действовавшими концепциями 1995 и 2001 годов. Одновременно развит ряд важ-

нейших направлений обеспечения национальной безопасности, использованы принципиально новые подходы.

Субъектами обеспечения национальной безопасности являются: государство, осуществляющее свои полномочия в данной сфере через органы законодательной, исполнительной и судебной власти; общественные и иные организации; граждане.

Объектами национальной безопасности являются: личность – ее конституционные права, свободы и законные интересы; общество – его материальные и духовные ценности, система общественных отношений, охраняемых нормами права; государство – его суверенитет, независимость, территориальная целостность, конституционный строй.

Выделены принципы обеспечения национальной безопасности, среди которых: законность, соблюдение конституционных прав и свобод человека; соблюдение баланса интересов личности, общества и государства, их взаимная ответственность; единство и взаимосвязь видов и направлений обеспечения национальной безопасности; разграничение сфер ответственности и полномочий государственных органов в решении задач обеспечения национальной безопасности; оперативность, своевременность, превентивность и соразмерность мер по нейтрализации источников внутренних угроз и защите от внешних угроз.

Обеспечение национальной безопасности осуществляется по направлениям, выделяемым в соответствии с основными сферами жизнедеятельности личности, общества и государства.

Производственная сфера должна быть ориентирована на создание совместных компаний по выпуску высокотехнологичной и сложнотехнической продукции, развитие сектора наукоемких услуг. Эффективным фактором решения поставленных задач должен стать экспорт капитала (технологий) в страны третьего мира, создание за рубежом сборочных производств по белорусским технологиям.

Одним из приоритетных направлений выступает повышение эффективности управления внешним долгом Республики Беларусь, снижение стоимости и рисков его обслуживания. Была закреплена задача вхождения в число первых 30 стран мира по условиям ведения бизнеса. По данным рейтинга Всемирного банка на 5 октября 2017 года Республика Беларусь занимает 37 место среди 190 государств. По показателю «подключение к системе электроснабжения»

Беларусь занимает наиболее высокую позицию (24-е место) среди государств-членов Евразийского экономического союза. Республика значительно улучшила свою позицию за счет внедрения системы «единого окна».

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Республики Беларусь. Национальная безопасность существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

Законодательство Республики Беларусь и ряда стран Содружества Независимых Государств (далее СНГ) в рассматриваемой сфере сориентировано на первоочередную защиту прав государства, а не индивида. В нормативной правовой сфере прослеживается четкая законодательная и фактическая тождественность «национальных интересов» «государственным интересам». При этом согласно статье 2 Конституции Республики Беларусь высшей ценностью и целью общества и государства является человек, его права, свободы.

Общество имеет право на получение информации в различных областях, которые интересны людям, в том числе по политическим вопросам, и средства массовой информации имеют право распространять эту информацию. Члены общества обладают также правом получать информацию о различных позициях и идеях, даже если они противоречат общим правилам. В соответствии с практикой Европейского суда по правам человека вмешательство государства в сферу деятельности средств массовой информации и свободы информации исключается.

Статья 34 Конституции Республики Беларусь гарантирует право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды.

Пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав.

Исходя из вышеизложенного, в Республике Беларусь можно выделить следующие системные противоречия в области пересечения национальной безопасности и прав человека:

– наличие недопустимых ограничений права на информацию как прямого продолжения права на свободу выражения мнений, в связи с использованием правовой системы для приоритетной защиты интересов государства в информационной сфере;

– недостаточный учет и использование международно-правовых стандартов и практически полное игнорирование европейско-правовых стандартов в сфере правового регулирования информационной безопасности;

– односторонняя и жесткая направленность законодательства на защиту прав государства как первоочередную задачу; интересы, права и потребности личности носят второстепенный и акцессорный характер;

– отождествление понятий «национальные интересы» и «государственные интересы»;

– слабая имплементация норм международных соглашений (за исключением соглашений в рамках СНГ) в национальное законодательство;

– присутствие основного массива международных соглашений Республики Беларусь в области обеспечения информационной безопасности в поле законодательства СНГ, большинство актов которого носит модельный (рекомендательный) характер либо не вступило в силу для отдельных государств-участников СНГ, либо не вступило в силу вообще;

– слабое развитие доктрины информационной безопасности и серьезное игнорирование при ее разработке международно-правовых теоретических, законодательных и правоприменительных стандартов (концептуально-научный уровень).

1. ЦИФРОВАЯ РЕВОЛЮЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Ускоренное создание и внедрение новых информационных технологий – «цифровая революция» – стало началом нового периода в развитии человечества к концу XX века. С одной стороны, этот процесс является естественным этапом научно-технического прогресса и необходимым условием дальнейшего развития общества: с каждым годом информационные технологии открывают все более широкие перспективы для повышения эффективности экономики и качества жизни людей. С другой стороны, дальнейшее развитие вычислительной техники и новых информационно-коммуникационных технологий (ИКТ) в XXI веке привело к закономерному процессу создания новых методов их применения в деструктивных целях, направленных против отдельных лиц, групп и, наконец, против структур управления государством, экономикой и вооруженными силами.

По выражению известного американского политолога Джозефа Ная: «Та страна, которая возглавит информационную революцию, и будет обладать большей силой по сравнению со всеми другими странами».

За 2016–2017 годы было создано больше информации, чем за всю историю человечества. И этот рост неуклонно продолжается. До 2020 года ожидается, что объем данных достигнет 44 зеттабайт (трлн гигабайт), увеличившись в 10 раз в сравнении с 2015 годом В 2017 году к Интернету подключился каждый второй житель Земли, и большая часть информации теперь фиксируется в электронном виде на устройствах, подключенных к Интернету.

Все это дает основание говорить о качественно новом уровне развития цифровых технологий, о новой фазе цифровой революции.

Подразумеваемые в наши дни под термином «цифровая революция» процессы базируются на таких предпосылках, как:

– экспоненциальный рост объемов информации;

– расширение и удешевление мощностей: вычислительных и хранения информации;

– прогресс в технологиях машинного обучения при анализе комплексных данных.

Информация становится доступной широкому кругу пользователей все в большем объеме и все оперативнее, в том числе рыночная –

в режиме реального времени. Всеобъемлющий онлайн-масштаб охватывает данные от котировок ценных бумаг и цен на товары для торговли и статистических оценок до спутниковых снимков, позволяющих анализировать перевозки транспортом, активность нефтяных вышек, прогнозировать погоду и т. п.

Интернет вещей вместе с расширением функциональных возможностей смартфонов, а также удешевление в сфере спутниковых технологий создает основу для аккумулирования все большего объема информации из зачастую ранее не существовавших источников. Треть информации к 2020 году будет проходить через облачные хранилища или находиться в них.

Накопление и доступность данных дополняется ростом возможностей по их обработке, структурированию, анализу. В качестве примера: ответ на поисковый запрос в Google формируется взаимодействием порядка 1000 компьютеров.

В итоге в ближайшие 20 лет до 50 % рабочих операций в мире могут быть автоматизированы, что сопоставимо с промышленной революцией XVIII–XIX вв.

Цифровая революция проявляется в:

– автоматизации все большего числа процессов;

– накоплении больших объемов данных у конкретных пользователей;

– доступе пользователей, в том числе онлайн, к массивам данных из внешних источников;

– новых методах и алгоритмах обработки значительных объемов данных, обеспечивающих недостижимые ранее результаты.

Цифровая революция несет в себе огромный потенциал для развития, но одновременно и серьезные вызовы, и риски.

Государственной безопасности цифровая революция может угрожать по следующим направлениям:

– кибертерроризм и кибершпионаж, ведущиеся странами и иностранными террористическими и преступными организациями, а также отдельными лицами и группами лиц;

– те же угрозы со стороны внутренних преступных сообществ, террористических организаций, радикальных религиозных, нацистских и прочих экстремистских группировок и антигосударственных сил;

– уход от налогообложения, незаконный вывоз капитала, отмывание преступно полученных доходов с использованием криптовалют;

– осуществление незаконной предпринимательской деятельности посредством использования сети Интернет, включая электронную торговлю и финансовые услуги.

Первая из перечисленных угроз наиболее серьезна и актуальна. США активно используют кибернетические средства ведущейся ими против России гибридной войны как основное в настоящее время наступательное оружие. Пока оно применяется для шпионажа и сбора информации, а также для дезинформации российского руководства и граждан посредством искусной работы в социальных и специальных сетях. Однако потенциально его разрушительное воздействие может иметь катастрофические последствия.

Следует заметить, что США являются единственной страной, выступающей против заключения международного договора по кибербезопасности. Они системно ведут электронный шпионаж по всему миру, в том числе против своих союзников. Обладая передовыми информационными технологиями и самым большим в мире парком информационно-вычислительного оборудования, фактической глобальной монополией в операционных системах, социальных сетях, доминирующим положением на рынке телекоммуникационных услуг и сложных электронных компонентов, США используют свое технологическое преимущество в политических и экономических целях. Отказываясь от подписания международного договора по кибербезопасности, они косвенно подтверждают намерение использования кибероружия и в дальнейшем.

Ключевым решением этой проблемы является заключение широкого международного соглашения по кибербезопасности, содержащего пункт о введении коллективных санкций стран-подписантов против государств, отказывающихся присоединяться к соглашению. Эти санкции могли бы включать:

– определение страны киберагрессором в случае выявления фактов ведения спецслужбами этой страны систематической деятельности по взлому или выведению из строя баз данных, интернет-сайтов, серверов, дата-центров, сетей управления органов государственной власти, объектов оборонного и стратегического значения, государственных корпораций, банков, объектов транспорта связи, энергетики, других систем жизнеобеспечения;

– перечень санкций, которые должны последовать в отношении страны, признанной в установленном порядке киберагрессором, введение эмбарго на импорт вычислительной техники, программного обеспечения, оборудования для нужд государства и государственных корпораций, отключение социальных сетей, прекращение телерадиовещания, прекращение банковских расчетов;

– коллективные действия по минимизации ущерба от введения санкций против киберагрессора. Они могли бы включать разработку и реализацию общего плана по импортозамещению, совместное создание средств программного обеспечения, общих социальных сетей, систем межбанковских расчетов, информационных сетей.

Нейтрализация второй группы угроз предполагает создание системы идентификации всех лиц, пользующих Интернет, включая социальные сети, а также специальной сертификации и тестирования оборудования для государственных нужд и стратегических объектов. Первая задача потребует соответствующего законодательного и административного обеспечения. Необходимо будет принять закон об обязательной добровольной идентификации пользователей Интернет, начиная с социальных сетей. Для его исполнения каждому пожелавшему себя идентифицировать гражданину должна быть предложена электронно-цифровая подпись и ключи для работы. Сети, отказывающиеся работать исключительно с идентифицировавшими себя гражданами, должны будут быть отключены от сегмента «всемирной паутины». Вторая задача носит технический характер, хотя тоже предполагает внесение соответствующих дополнений в законодательство о государственных закупках.

После решения задачи идентификации всех работающих в сетях лиц нейтрализация третьей и четвертой групп угроз не будет представлять принципиальной сложности. Для этого у налоговой службы, финмониторинга Банка имеется достаточно технических возможностей и компетенций.

Серьезной угрозой общественной безопасности считается рост безработицы в связи с роботизацией рабочих мест, автоматизацией управленческих процессов, растущим применением 3D-принтеров. Но, как показывает почти трехсотлетний опыт современного промышленного развития, эта угроза частично нейтрализуется другими факторами.

Во-первых, наряду с застойной безработицей в одних отраслях, всегда есть нехватка рабочей силы в других. Дисбаланс на рынке труда резко обостряется в период смены технологических укладов. В это время экономика погружается в депрессию в связи с прекращением расширения экономики в сложившихся направлениях, сокращением производства и инвестиций в отраслях, обеспечивавших в течение двух поколений трудоспособного населения основной рост занятости.

Во-вторых, роботизация, как и цифровая революция в целом, уже давно идет, уничтожив сотни миллионов мест в различных отраслях промышленности. С 80-х годов прошлого века с ростом нового на тот момент информационно-коммуникационного технологического уклада автоматизация производства охватила множество отраслей обрабатывающей промышленности. Гибкие производственные линии сделали ненужным труд миллионов сборщиков, расфасовщиков, станочников. Жесткая автоматизация конвейерных производств высвободила еще миллионы людей, занятых монотонным трудом по выполнению простых рутинно повторяющихся операций. Прогресс в вычислительной технике ликвидировал миллионы рабочих мест машинистов, перфораторщиков, нормировщиков, проектировщиков, бухгалтеров и рабочих мест по другим специальностям, связанным с рутинными расчетами по установленным алгоритмам. Десятки миллионов замещаемых автоматикой людей оказались в трудном положении, но социального бедствия, подобного Великой депрессии, когда происходила предыдущая смена технологических укладов, не произошло. Молодежь с энтузиазмом освоила новые профессии программистов, операторов, наладчиков. Пожилые люди досрочно ушли на пенсию. Многие нашли себя в сфере услуг, быстрое расширение которой стало наиболее заметной стороной роста нового технологического уклада, породив разговоры о переходе к постиндустриальному этапу экономического развития. На самом деле промышленность по-прежнему является основой современной экономики, только на рынке труда ее доля резко снизилась в среднем до 25 % в передовых странах.

В-третьих, в обозримом будущем спрос на специалистов, необходимых для создания инфраструктуры цифровой экономики будет намного больше, чем связанное с ее расширением уничтожение рутинных рабочих мест, но только в том случае, если цифровая экономика будет развиваться на отечественной интеллектуально-

технологической базе. Если проводимая государством политика в сфере информационных технологий не изменится и в ее основе будет лежать импорт техники и программного обеспечения, то эффект может оказаться и сильно отрицательным.

Политической проблемой может стать использование цифровых технологий в сфере государственного контроля. К примеру, применение технологии блокчейн сделает невозможным фальсификацию регистрационных документов, подделку разрешительных документов, переделку «задним числом» проверочных актов. Эта технология также делает ненужной значительную часть дорогостоящих нотариальных услуг по заверению сделок. Применение «умных контрактов» затруднит чиновный произвол в сфере государственных закупок. Использование электронной цифровой подписи и методов точной идентификации бумажных и электронных носителей исключит подделку документов. Вся система государственного управления станет более прозрачной и открытой для общественного контроля. Сократится коррупционное поле и снизится потребность в чиновниках контролирующих органов.

Наконец, последняя группа угроз, связанная с риском для человечества в целом. Современная наука вплотную подошла к разработке технологий изменения человеческой природы, и угроза опасных для человечества последствий цифровой революции действительно существует. Разберем их по порядку потенциально актуализации:

– угроза использования генно-инженерных технологий для создания опасных для человека микроорганизмов. Она давно существует и явно недооценивается органами национальной безопасности. Уже два десятилетия назад ученые признавали возможность синтезирования вирусов избирательного действия против людей, групп людей с определенными биологическими признаками. Комбинируя ДНК живущих в симбиозе с человеком вирусов с патогенными, можно синтезировать вирусы, вызывающие болезни у людей определенного пола, возрастной группы и даже расы. Доставляя эти вирусы посредством экспорта продуктов питания на территорию враждебной страны, можно вызвать в ней эпидемии и обойти таким образом обоюдоострый характер биологического оружия. По-видимому, такие исследования в лабораториях США ведутся вопреки запрету биологического оружия. Во всяком случае, лидеры некоторых африканских стран искренне считают Вашингтон виновным в создании и распространении лихорадки Эбола;

– клонирование людей, в том числе с определенными свойствами. Об этой угрозе ученые заговорили более десятилетия назад, когда экспериментально была доказана возможность клонирования млекопитающих и открылись практические возможности клонирования высших приматов и человека. Сегодня клонирование собак стало поставленным на поток коммерческим предприятием и теоретически возможно появление фабрик по клонированию людей;

– вживление в людей различных кибернетических устройств. Это уже хорошо освоенная технология в медицине, широко использующей кардиостимуляторы, слуховые аппараты, протезы, датчики. Теоретически возможно появление киборгов – людей со встроенными в их организм приборами в целях наделения их дополнительными вычислительными способностями, улучшения работы их органов чувств, идентификации личности, передачи им информации, манипулирования поведением и прочее;

– включение человеческих органов и их моделей в робототехнические устройства. Это пока такая же фантастика, как голова профессора Доуэля в романе Беляева. Но разработки моделей нервной системы человека интенсивно ведутся и вполне возможно появление наделенных элементами человеческого образа андроидов, а также роботов с искусственным интеллектом;

– выход из-под контроля способных к самоорганизации автономных роботомашинных систем. Бунт роботов из художественного теоретически может превратиться в реальный кошмар недалекого будущего. Уже сегодня сбои автоматизированных систем электроснабжения повергают в хаос крупные города. Если системы искусственного интеллекта смогут самоорганизовываться и принимать самостоятельные решения, последствия предсказать невозможно.

Все перечисленные выше угрозы существованию человечества хорошо известны и многократно обсуждались. Однако реальных предложений по их нейтрализации пока не выработано. Очевидно, что научно-технический прогресс остановить невозможно, несмотря на его опасные для человечества последствия. Но общество может ограничить его рамками права. Чтобы быть действенными, эти ограничения должны носить международный характер и охватывать все страны с существенным научно-техническим потенциалом.

Для избегания больших угроз будет целесообразней принимать международные договоры, необходимые для ограничения охарактеризованных выше опасных направлений развития цифровых технологий. В том числе, предусматривающие:

– запрет на проведение клонирования людей;

– запрет на разработку болезнетворных вирусов и иных форм биологического оружия;

– введение международных стандартов вживления приборов в тело человека;

– мониторинг разработок систем искусственного интеллекта с целью диагностики и нейтрализации угроз для человечества;

– всемирную сертификацию специалистов, получающих образование в сфере информационных технологий;

– разработку и принятие международных технических регламентов и процедур сертификации роботов-андроидов.

Цифровая революция активно внедряется во все области человеческой деятельности, в том числе и в экономику. Цифровая экономика стремительно вытесняет старый уклад во всех сферах деятельности современного общества. Трансформируется частная жизнь и рабочие места, появляются новые профессии и инструменты взаимодействия. Благодаря цифровой экономике повышается эффективность всех отраслей за счет использования информационных технологий; качественно и количественно увеличиваются возможности совершения через компьютер практически всех операций, среди которых предоставление/получение различных услуг и выполнение транзакций. Однако, помимо ряда преимуществ, цифровая трансформация несет и определенные риски. Жизненно важные интересы субъектов (государства, юридических и физических лиц), участвующих в процессах автоматизированного взаимодействия, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальные коммерческие и персональные данные были бы постоянно легко доступны и в то же время надежно защищены от неправомерного использования. Искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи, наносят серьезный материальный и моральный

урон. Таким образом, крайне остро встает вопрос обеспечения информационной безопасности как различных госструктур, так и персональных данных и коммерческих организаций.

В Беларуси утверждена Государственная программа развития цифровой экономики и информационного общества на 2016–2020 годы. Соответствующее решение закреплено постановлением Совмина от 23 марта 2016 года № 235. Предполагается, что программа должна стимулировать «ускоренное развитие инновационных секторов экономики» и привлечение эффективных инвестиций. В числе главных целей и задач – быстрое развитие высокотехнологичных производств и услуг, формирование благоприятной бизнес-среды, рост экспорта. Программа включает три основных направления развития цифровой экономики:

1. Информационно-коммуникационная инфраструктура.
2. Инфраструктура информатизации.
3. Цифровая трансформация.

Переход к цифровой экономике должен сопровождаться обеспечением комплексных мер безопасности. Об этом говорилось на открытии IT-форума 7 июня 2017 года в г. Ханты-Мансийске, где состоялась 1-я Международная конференция по информационной безопасности с участием стран БРИКС, ШОС и ОДКБ «Инфофорум-Югра». В ее работе приняли участие представители Армении, Беларуси, Бразилии, Вьетнама, Казахстана, Малайзии, Российской Федерации и ЮАР. Форум прошел под девизом «От информационных технологий к цифровому обществу». Основное внимание было уделено проблемам информационной безопасности, переходу к цифровой экономике, демонополизации мирового рынка компьютерного оборудования и программного обеспечения, развитию импортозамещения, формированию эффективной системы государственного управления информатизации здравоохранения.

Формирование цифровой экономики – это вопрос национальной безопасности и независимости. Цифровая экономика – это не отдельная отрасль, а уклад жизни, новая основа для развития экономики, бизнеса, социальной сферы.

Необходимо отметить, что одним из приоритетов является защита персональных данных физических лиц. Эти вопросы не остаются без внимания законодательных и правоохранительных органов всех государств.

25 мая Европейский союз официально перешел на новые правила обработки персональных данных GDPR (Общий регламент по защите данных ЕС 2016/679 от 27 апреля 2016 года). Важной особенностью GDPR является экстерриториальный принцип действия, он затрагивает все компании, обслуживающие потребителей в ЕС. Штрафы могут достигать €20 млн или 4 % дохода компании на мировом рынке за год. Для обычных пользователей внешне мало что изменится: как правило, придется снова принять различные соглашения об обработке своих персональных данных, зато защита последних предусмотрена на гораздо более серьезном уровне.

Под персональными данными в GDPR подразумевается любая информация, относящаяся к физическому лицу, по которой можно прямо или косвенно его идентифицировать. То есть речь может идти об имени, данных о местоположении, онлайн-идентификаторе и прочих факторах вроде IP-адреса, помогающих установить личность. Есть и особые конфиденциальные персональные данные: расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, генетическая и биометрическая информация, сведения о состоянии здоровья, сексуальной жизни.

Основные принципы обработки персональных данных по GDPR:

– персональные данные должны обрабатываться законно, справедливо и прозрачно, причем любую информацию о целях, методах и объемах обработки персональных данных компании обязаны излагать максимально доступно и просто;

– данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией или службой;

– нельзя собирать личные данные в большем объеме, чем необходимо для целей обработки;

– неточные личные данные должны быть удалены или исправлены по требованию пользователя;

– личные данные должны храниться только в той форме и на тот срок, который позволяет идентифицировать человека в заявленных целях обработки;

– при обработке персональных данных компании обязаны обеспечить их защиту от несанкционированного или незаконного доступа, уничтожения и повреждения.

GDPR требует, чтобы согласие пользователя на обработку его персональных данных было выражено в форме утверждения или в форме четких активных действий. Кроме того, согласие может считаться недействительным, если у пользователя не было возможности отозвать его без ущерба для себя.

Для компаний, которые действовали по принципу извлечения максимума информации о пользователях для последующего возможного анализа, реорганизация в рамках GDPR во многом может оказаться пыткой: ведь нужно удалить лишнюю информацию, оставив лишь самую необходимую для текущих задач.

Но, возможно, самым серьезным требованием GDPR является право на запросы доступа к персональным данным. Пользователи из ЕС могут запрашивать удаление информации, исправлять ее, если она неверна, и даже получать ее в удобном для переноса виде. Но эти данные могут быть на пяти разных серверах в массе различных форматов. Другими словами, переход на стандарты GDPR требует создание внутренней инфраструктуры, позволяющей эффективно обрабатывать запросы пользователей.

Несмотря на то, что новые требования к обработке персональных данных серьезны, в них есть положительные стороны для внеевропейских игроков: легче придерживаться единого набора правил защиты и обработки данных, чем учитывать национальные нюансы обработки персональных данных каждой отдельной страны ЕС, как это приходилось делать до введения GDPR. Более того, реформа направлена на стимулирование экономического роста путем сокращения расходов и бюрократии для компаний, работающих в ЕС. Соблюдение одного правила вместо 28 (количество стран-членов ЕС) поможет маленьким и развивающимся компаниям выйти на новые рынки. Согласно закону в ряде случаев обязательства изменяются в зависимости от размера бизнеса, природы обрабатываемых данных и иных факторов.

GDPR – важнейший законодательный документ, который существенно повышает уровень защиты персональных данных в ЕС и за его пределами. Он требует очень внимательного изучения и соблюдения. Реформа дает ясность и последовательность правил, которые должны применяться в области защиты данных. Она также восстанавливает доверие пользователя-потребителя, что позволяет бизнесу максимально использовать возможности на едином европейском

цифровом рынке. Сбор, анализ и перемещение персональных данных по всему миру приобрели огромное экономическое значение. Персональные данные – это, безусловно, «валюта» современной экономики. И если вы осуществляете сбор пользовательских данных в каком-либо виде – за их сохранностью надо внимательно следить, чтобы избежать утечек и возможных манипуляций ими третьими лицами.

Важнейший фактор постоянно расширяющегося внимания к проблемам информационной безопасности – развитие рисков и угроз в информационной сфере с внедрением в жизнь цифровой экономики, высоких технологий, электронных услуг во всех сферах повседневной жизнедеятельности граждан. Особенно заметно рискам подвергается население в связи с широким распространением Интернета, социальных сетей, повсеместным использованием мобильных устройств. Под угрозой находятся интересы миллионов пользователей информационно-коммуникационных технологий.

Вопросы для самоконтроля

1. Понятие «цифровой революции».
2. Основные угрозы государственной безопасности, связанные с «цифровой революцией».
3. Меры противодействия угрозам государственной безопасности.

2. КИБЕРБЕЗОПАСНОСТЬ И КИБЕРВОЙНЫ

С развитием технологий и проникновением Интернета во все сферы деятельности человека, в мире появились такие понятия как кибербезопасность и кибервойны.

Кибербезопасность – раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности. Под киберобъектом здесь понимается любой объект, функционирование которого осуществляется с участием программируемых средств.

Кибервойна – это особый род противостояния в сети интернет, который направлен на подрыв нормального функционирования соответствующих систем в государственных органах, финансовых организациях, почтовых службах и иных предприятиях, активно использующих данный вид связи. Для проведения подобных военных действий необходимо только одно оружие – персональный компьютер, подключенный к глобальной сети и квалифицированный человек, который сидит за монитором.

Методики кибервойны заключаются в проведении направленных хакерских атак на определенные ключевые элементы в государственных структурах и управляющие элементы, которые отвечают за нормальное функционирование водоснабжения, распределение электроэнергии, транспортных потоков, энергоресурсов и связь.

В связи с широчайшим распространением информационных технологий во всех сферах нашей жизни подобная подрывная деятельность в случае успеха может нанести ущерб, который будет сопоставим со взрывом нескольких атомных бомб. Таким образом, можно дезориентировать и деморализовать противника, не применяя обычных средств вооружения и не вводя на территорию враждебного государства ни одного солдата.

Задача такого рода войны – достичь определенных целей в экономической, политической, военной и других областях посредством влияния на общество и власть тщательно подготовленной информацией. В связи с этим, войну нового времени можно назвать психо-

логической. Кибервойна является одной из разновидностей информационной войны и представляет собой противостояние в кибернетическом пространстве. Компьютерные технологии и Интернет получили широкое распространение по всему миру и используются не только в повседневной жизни граждан, но и на предприятиях, в государственных учреждениях, которые, в свою очередь, являются важной структурной единицей страны. Манипуляция «противником» данными, полученными из подобных мест, представляет угрозу для национальной безопасности стран.

Высоким приоритетом информационной войны является не только нанесение ущерба противнику, но и защита собственных данных, поэтому кибербезопасность – неотъемлемая часть подобного рода противостояний. Она представляет собой совокупность принципов, средств и стратегий для обеспечения неуязвимости и защиты киберсреды, а именно доступность, целостность и конфиденциальность данных.

Цель и этапы ведения кибервойны

Кибернетическая война состоит из двух этапов: шпионаж и атаки. Первый этап подразумевает сбор данных посредством взлома компьютерных систем других государств. Атаки можно разделить в зависимости от цели и задач военных действий.

Вандализм – размещение пропагандистских или оскорбительных картинок на веб-страницах вместо исходной информации.

Пропаганда и информационная война – использование пропаганды в контенте веб-страниц, в рассылках обращений.

Утечки конфиденциальных данных – все, что представляет интерес, копируется со взломанных частных страниц и серверов, также секретные данные могут быть подменены.

DDoS-атака – атака с нескольких машин с целью нарушить функционирование сайта, системы компьютерных устройств.

Нарушение работы компьютерной техники – атаке подвергаются компьютеры, отвечающие за функционирование оборудования военного или гражданского назначения. Атака приводит к выходу из строя техники или к ее отключению.

Примером может служить вирус Stuxnet.

Время создания вируса Stuxnet. Главная задача вредоносной программы заключалась в замедлении ядерных разработок Ирана,

вплоть до нанесения вреда реакторам, что могло привести к заражению огромных территорий. Считается, что это кибероружие, разработанное специалистами США и Израиля. Stuxnet работал постепенно и незаметно, увеличивая скорость вращения ядерных центрифуг, которые поддерживали завод, медленно разрушая их. В 2010 году, когда проблема была обнаружена, Stuxnet уже уничтожил пятую часть всех ядерных центрифуг в Натанзе. Катастрофу удалось предотвратить, но избавиться от проблемы не получилось. Более того, сейчас он распространился по всему миру. Учитывая известную о вирусе информацию, можно предположить, что после команды «сверху» тот способен парализовать работу любых предприятий, где в управлении используются компьютеры.

Атака инфраструктурных и критически важных объектов и кибертерроризм – воздействие на машины, регулирующие инженерные, телекоммуникационные, транспортные и другие системы, обеспечивающие жизнедеятельность населения.

Все действия кибервойны направлены на нарушение функционирования вычислительных систем, отвечающих за работу деловых и финансовых центров, государственных организаций, создание беспорядка в жизни страны, поэтому в первую очередь страдают важные жизнеобеспечивающие и функциональные системы населенных пунктов. К ним относится система водоснабжения, канализация, электростанции, энергетические узлы, другие коммуникационные сети.

Зависимость госучреждений, предприятий и простых граждан от интернета значительно возросла. При этом кибератаки одного государства, направленные против другого, могут нанести весомый ущерб экономике страны. Кибервойна является реальной угрозой для безопасности страны. Ведь создать компьютерный вирус или троян обойдется значительно дешевле, в сравнении с покупкой оружия и ракет. При этом урон, нанесенный от кибервторжения, может превзойти все самые смелые ожидания.

Специалисты делят киберпространство на три уровня:

– *физический* – к этому уровню относится сетевое оборудование, кабели и инфраструктура;

– *семантический* – всевозможные необработанные данные, которые передаются в сети;

– *синтаксический* – связующее звено между первым и вторым уровнем.

Кибератаки разделяют на:

– *семантические* – при этом уничтожаются, меняются или похищаются данные;

– *синтаксические* – направлены на нарушение потоков передачи данных, для этого используются вредоносные программы;

– *физические* – кибератаки реальных инфраструктурных объектов.

Понятие «кибервойна» тесно связано с понятием «кибербезопасность». Кибербезопасность являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Кибербезопасность является необходимым условием развития информационного общества.

Многие страны мира, среди которых РФ, США, Китай и Израиль, создают специальные киберподразделения, главная задача которых заключается в массированных компьютерных атаках противника, а также защите собственных сетей от такого же внешнего воздействия. Современная война может начаться с одного вируса, который уничтожит инфраструктуру врага без единого выстрела, сразу же поставив точку в противостоянии.

Подходы стран к кибербезопасности

В годы «Холодной войны» всю информацию о достижениях зарубежной науки и техники, равно как и обо всех остальных сферах общественной жизни, граждане СССР получали, в основном, через призму советского телевидения и радио. Соответственно, было довольно трудно составить объективную картину происходящего в мире. Сегодня все изменилось. Для того чтобы разобраться в любом вопросе с разных сторон, нужно просто иметь подключение к интернету, обладать незаурядными навыками поиска в сети и знать иностранные языки.

Рассмотрим подходы ряда зарубежных государств к кибербезопасности.

Кибербезопасность в США

«У нас нет плана» – именно такую точку зрения высказал один очень известный и уважаемый американский журналист Тэд Коппел в своей книге «Погасить огни: кибератака и борьба с последствиями». Он говорит о том, что катастрофические последствия урагана Sandy, который обрушился в октябре 2012 года на восточное побережье США, могут показаться цветочками по сравнению с кибератакой извне на энергетические сети. «У нас есть план на случай землетрясения, у нас есть план на случай урагана, у нас есть инструкции на случай наводнения, но у нас, увы, нет плана на случай кибератаки».

В разговоре с журналистом секретарь совета безопасности Джей Джонсон сказал, что вероятно такой план существует и его совсем не обязательно показывать общественности. Людям просто достаточно иметь радио на батарейках, чтобы в случае форс-мажора настроиться на нужную волну и прослушать инструкции.

При этом экс-министр обороны Леон Панетта предупреждал об опасности цифрового Перл-Харбора еще в 2012 году, а президент США упоминал об опасности кибератак в двух своих последних посланиях к нации. Несмотря на это в правительственных кругах нет никаких признаков беспокойства.

По словам Тэда Коппела, единственная социальная группа, которая готова к любой катастрофе, в том числе и в киберпространстве, это мормоны в Солт-Лейк-Сити. И то, только потому, что они возвели неизбежность катастрофы в культ и живут с этой мыслью.

Для рядовых американцев кибератака из-за рубежа представляется чем-то эфемерным и не заслуживающим внимания. Таковы особенности их национального менталитета: все, что происходит за океаном и не касается их лично, – не важно.

Судя по данным из официальных докладов, только за 2014 год против федеральных структур в США было совершено более 60 тысяч кибератак. Понятно, что не все инциденты имели далеко идущие последствия. Но, очевидно, взлом базы данных Федерального управления персоналом (Office of Personnel Management), которое отвечает за подбор сотрудников в государственные ведомства США, и в результате которого в руки злоумышленников попали личные данные 4-х миллионов американцев, представляет серьезную опасность для национальной безопасности.

Американцы обвинили в этой атаке Китай, не предоставив никаких субстантивных доказательств.

Авторитетный американский политолог Ян Бремер в статье для журнала Time говорит, что в 21 веке банальный грабеж на волне новых технологий плавно перешел в киберпространство. По данным ФБР об атаках в 2013 году заявили более 3000 компаний от средних банков, до крупных оборонных предприятий. Причем действия хакеров стоят американскому бизнесу в районе $ 300 млн ежегодно.

Согласно подходам США, основная угроза в киберпространстве для Вашингтона исходит из Китая, потому что китайские хакеры в большей степени занимаются кибершпионажем и банальным воровством интеллектуальной собственности. Причем речь идет о целых группах хакеров, которые щедро спонсируются государством.

Китай на определенном этапе решил активно развивать свои кибервозможности и, судя по оценкам американских экспертов и официальных лиц, серьезно преуспел в этом. Многие были свидетелями «новинок» китайского автопрома, фантастически похожих на продукцию американских и европейских автоконцернов. То же самое касается и военной техники, крылатых ракет, систем ПВО, самолетов и многого другого. Неслучайно новый китайский истребитель Chengdu J-20 так сильно похож по дизайну на американский F-22 Raptor, а Shenyang J-31 – практически точная копия F-35.

Киберугрозы из Российской Федерации

Говоря о киберугрозах, исходящих из России, американские эксперты и некоторые зарубежные лидеры чаще всего приводят в качестве примера масштабную DDoS-атаку против эстонских правительственных ресурсов в 2007 году, а также кампанию в соцсетях в контексте украинского кризиса.

Президент Эстонии Тоомас Хендрик Ильвес в ходе выступления в центре им. Вудро Вильсона (Вашингтон) в апреле 2015 года отметил успехи Москвы на ниве ведения информационной войны и назвал противостояние вокруг Украины «эпоха Dezinformatsiya 2.0». По словам эстонского президента, еще в 80-е годы прошлого века была известна «тактика придумывания какой-нибудь истории, которая попадала в Hindustan Times, затем ее перепечатывали где-нибудь в Италии и, наконец, она оказывалась на страницах New York Times».

Известный журналист Эдриан Чен в New York Times провел целое расследование о российском информационном ноу-хау: интернет-троллях из Агентства интернет-исследований в Санкт-Петербурге. Судя по его материалу, сотрудники этой организации или «тролли» в ежедневном режиме публикуют более 100 комментариев на сайтах СМИ, ведут несколько аккаунтов в социальных сетях и обязаны публиковать до 50 информационных сообщений ежедневно. По мнению журналиста, именно это Агентство и является источником масштабной кампании по дезинформации в контексте украинского кризиса.

Киберстратегия Пентагона

В конце апреля 2015 года Пентагон презентовал новую стратегию кибербезопасности, которая явилась неким расширенным вариантом аналогичного документа от 2011 года.

Выделяется три основных направления деятельности в этой сфере.

Первое – защита собственных информационных систем от хакерских атак извне.

Второе – работа с другими агентствами и зарубежными союзниками по сбору информации разведывательного характера, совместные операции с ФБР, ЦРУ, АНБ и иностранными спецслужбами вплоть до создания системы автоматического обмена информацией, а также создание особой оперативной группы по кибербезопасности в Стратегическом командовании США.

Третье направление – кибернетическая поддержка военных операций США и привлечение квалифицированных гражданских специалистов.

Новый документ в отличие от своего предшественника прямо называет основных противников США в киберпротивоборстве: КНР, Россия, КНДР и Иран. Причем упоминаются и негосударственные акторы, вроде хакеров из ИГИЛ (запрещенная в России террористическая организация) и преступных синдикатов.

Вместе с тем, остаются в силе и стратегические цели прошлой киберстратегии от 2011 года:

– создание и поддержка боеготовности сил и возможности проводить операции в киберпространстве;

– обеспечение защиты военных сетей;

– укрепление межведомственного сотрудничества для противодействия киберугрозам;

– усиление международного сотрудничества в сфере кибербезопасности.

Таким образом, будет увеличиваться финансирование киберподразделений в армии и спецслужбах США, будет интенсифицироваться подготовка гражданских специалистов в этой отрасли и их рекрутирование, будет вестись работа на данном направлении с союзниками по НАТО.

Американцы, обозначив в качестве своих противников КНР, Россию, Иран и КНДР, таким образом, официально признали, что против этих государств проводятся и будут проводиться в будущем кибероперации. Также, США, признавая эффективность так называемой «гибридной войны», одним из элементов которой как раз и являются боевые действия в киберпространстве, будут наращивать усилия на данном направлении.

Кибербезопасность в Российской Федерации

В Российской Федерации в 2016 году была принята новая доктрина информационной безопасности. Эксперты долгое время настаивали на том, что старая доктрина (2000 года) сильно устарела и не отвечает стремительно меняющейся реальности.

В России кибербезопасность является неоформленным четко разделом большой доктрины по информационной безопасности и поэтому рассматривается именно в этом контексте, несмотря на попытки ряда сенаторов утвердить отдельную киберстратегию, которая бы касалась исключительно интернет-пространства. По слухам, против выступила Федеральная служба безопасности, сославшись на некорректность термина «кибербезопасность».

В связи с этим, велись споры и в экспертном сообществе, и на межведомственном уровне о том, в какую же сторону пойти. Решили, что стоит оставить понятие «информационная безопасность» и объединить все в это понятие.

Новая доктрина информационной безопасности Российской Федерации констатирует, что киберпространство все чаще используется «для решения военно-политических задач, а также в террористических и иных противоправных действиях».

При этом обозначены пять блоков киберугроз:

– воздействие иностранных государств на критическую информационную инфраструктуру РФ (системы энергообеспечения, управления транспортом, водоснабжения и т. д.);

– использование спецслужбами иностранных государств и подконтрольными общественными организациями киберпространства для подрыва суверенитета и дестабилизации социально-политической обстановки в России;

– рост масштабов киберпреступности;

– отставание России в сфере разработки собственного программного обеспечения;

– использование отдельными государствами технологического доминирования в глобальном информационном пространстве для достижения экономического и геополитического преимущества.

Для противодействия перечисленным киберугрозам Россия планирует работать в правовой сфере с зарубежными партнерами, развивать свои силы и средства информационного противоборства, а также пытаться создать систему стратегического сдерживания и предотвращения военных конфликтов.

В мае 2015 года был подписан ряд соглашений между Москвой и Пекином в области информационной безопасности, который сейчас именуют как «пакт о киберненападении».

Сложно говорить о том, кто конкретно стоит за кибератаками, которые западные СМИ и зарубежные политики приписывают России. Это могут быть и спонсируемые государством хакерские группировки, и соответствующие подразделения в спецслужбах, и самостоятельные кибервзломщики.

Однако можно говорить с уверенностью, что российские хакеры являются большими профессионалами в своем деле. Одни только заголовки западных ведущих СМИ чего стоят: «Русские хакеры обрушили DowJones», «Русские хакеры атаковали Пентагон и Белый дом», «Русские хакеры атаковали личный сервер Хилари Клинтон», «Русские хакеры получили доступ к коммерческим спутникам».

Кибербезопасность в Китае

«Воевать без оружия, побеждать без боя» – это высказывание, принадлежащее древнекитайскому мыслителю Сунь-Цзы, в полной

мере отражает подход КНР к информационной безопасности. В Китае, как и в России, пока не прижился термин кибербезопасность, поэтому понятийный аппарат в целом похож на российский: информационная безопасность, информационная сфера, информационные угрозы.

Китайское военно-политическое руководство отдает себе отчет в том, что в случае прямого военного противостояния с США народно-освободительная армия Китая (НОАК) не сможет противостоять хорошо вооруженному и подготовленному заокеанскому противнику. Поэтому ставку сделали на развитие киберподразделений и экономический кибершпионаж.

Существуют оценки, согласно которым Пекин при желании может организовать хакерскую атаку такой силы, что США перестанут существовать как государство. Однако узнать, действительно ли в Китае дела обстоят таким образом, можно лишь после осуществления атаки. Но в одном можно быть уверенным на сто процентов: Китай инвестирует в развитие киберпространства и киберподразделений своих вооруженных сил миллиарды юаней.

Стоит отметить, что Китай – фактически пионер в области регулирования Интернета: такой цензуры и такой закрытости национального информационного пространства нет больше нигде в мире.

Известные события на площади Тяньаньмэнь в 1989 году (серия демонстраций в КНР, продолжавшаяся с 15 апреля по 4 июня). Главными участниками выступлений были студенты, которые требовали от властей ответа: почему обещанные политические реформы отстают от экономических. Количество митингующих увеличивалось, к студентам присоединялись рабочие, служащие, бизнесмены и даже полицейские. Интеллектуалы полагали, что правительство погрязло в коррупции и управляет страной тоталитарными методами, рабочие считали, что реформы в Китае зашли слишком далеко и возникшая в результате высокая инфляция и безработица угрожает им и их семьям. Последовавшая за этим демонизация образа китайской компартии в западных СМИ поставила руководство Китая перед выбором: позволить информационно-коммуникационным технологиям бесконтрольно развиваться или закрыть доступ населения к ним.

В итоге выбрали нечто среднее и создали так называемый великий китайский файрвол. Эта система позволила оградить Китай от

всемирной паутины, а заодно и от посягательств иностранных хакеров. При этом в поднебесной активно используют интернет для развития экономики, образования, медицины, формируют систему электронного правительства и даже создали свои аналоги Twitter, Facebook и Instagram.

При этом интернет в Китае вовсе не диковинка, как может показаться извне. Согласно данным ряда отечественных исследователей, уже в 2009 году около 90 % китайских городов и поселков имели высокоскоростной доступ в интернет, а 92,5 % деревень могли подключиться к сети по телефонной линии.

Однако стать пользователем Интернета в Китае не так просто. Для этого нужно сначала пройти регистрацию в полицейском участке и предоставить интернет-провайдеру соответствующую справку. Есть неофициальная информация, что в руководстве всех провайдеров сидят полицейские, которые постоянно отслеживают обстановку в сети. Любой ресурс, который замечен в публикации материалов, дискредитирующих политику компартии, закрывается без лишних церемоний с жесткими «оргвыводами» для владельцев сайта.

Таким образом, подход Китая к обеспечению кибербезопасности в общих чертах совпадает с оценками западных экспертов: хакерские атаки и кибершпионаж против стран Запада, Японии, Южной Кореи и, вполне возможно, России имеют место быть. Они совершаются либо окологосударственными хакерскими группами, либо подразделениями НОАК (деятельность самостоятельных хакеров практически полностью исключается из-за особенностей местного интернет-законодательства). Впоследствии информация, которая добывается кибервоинами, передается в промышленность.

Когда происходит хакерская атака против какой-то компании, всегда важно понять, кто является ее заказчиком и исполнителем. Только при наличии соответствующих доказательств можно идти в суд или прокуратуру и требовать с обидчика возмещения ущерба.

Когда мы говорим о хакерских атаках на государственном уровне, то сталкиваемся с тем, что доказать причастность той или иной страны к кибернападению крайне трудно. А значит, при соблюдении надлежащих требований безопасности участники этой многосторонней кибервойны могут делать все что угодно. Правил в этой виртуальной драке нет.

Сегодня, в эпоху гаджетов, девайсов и повсеместного интернета, человечество может оказаться на пороге глобальной кибервойны, где решать исход битвы будут не танки с артиллерией и даже не стратегические бомбардировщики с подводными лодками, а подразделения молодых кибервоинов с мощными компьютерами и разрушительными вирусами на флешках.

Кибербезопасность в Беларуси

Глобальный индекс кибербезопасности (GCI) отражает уровень киберзащищенности государств и усилия, которые прилагает страна для улучшения этого показателя. Среди критериев: правовое, техническое, организационное поля, а также потенциал и сотрудничество.

В индексе 2017 года Беларусь заняла 39 место в мире и третье среди стран СНГ – после Грузии и России. Республика обходит по уровню кибербезопасности Литву, Казахстан, Кыргызстан, Азербайджан, Украину и многие другие страны.

Среди мировых лидеров по уровню кибербезопасности – Сингапур, США, Малайзия, Эстония и Оман.

По сравнению с предыдущим годом, Беларусь поднялась в рейтинге относительно других государств постсоветского пространства. Самая слабая сторона республики в кибербезопасности, по мнению составителей рейтинга, – в уровне сотрудничества с компонентными органами других стран.

Вопросы для самоконтроля

1. Понятия «кибервойна» и «кибербезопасность».
2. Цель и этапы ведения кибервойны.
3. Кибербезопасность в США.
4. Кибербезопасность в Российской Федерации.
5. Кибербезопасность в Китае.
6. Кибербезопасность в Беларуси.
7. Киберстратегия Пентагона.
8. Киберугрозы из Российской Федерации.

3. НОРМАТИВНО-ПРАВОВАЯ БАЗА РЕСПУБЛИКИ БЕЛАРУСЬ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Правовое обеспечение информационной безопасности представляет собой деятельность законодательных и исполнительных органов государственной власти по разработке, реализации и контролю исполнения совокупности нормативных правовых актов, регламентирующих практическую деятельность по защите информации личности, общества и государства.

Правовое обеспечение информационной безопасности направлено на:

– обеспечение эффективной реализации и защиту конституционных прав личности;

– неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства;

– создание благоприятных условий для свободного и оперативного доступа к информации органов государственной власти и органов местного самоуправления, непосредственно затрагивающей права и свободы личности;

– защиту прав участников электронной коммерции;

– защиту интеллектуальной собственности;

– обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом;

– защиту интересов государства и общества в сфере использования государственных информационных ресурсов и т. д.

Правовое обеспечение призвано создавать и поддерживать в обществе негативное отношение к нарушителям информационной безопасности и, в частности, сформировать карательные меры воздействия к злостным нарушителям.

Нормативно-правовую базу в области информационной безопасности в Республике Беларусь составляет «Концепция национальной безопасности Республики Беларусь», законы Республики Беларусь «Об информации, информатизации и защите информации», «О государственных секретах», «Об электронном документе». Отдельные правовые нормы по вопросам защиты информации содержатся

в Гражданском и Уголовном кодексах Республики Беларусь, указах Президента, постановлениях Совета Министров, руководящих документах Национального банка, нормативных правовых актах министерств и иных республиканских органов государственного управления.

Основополагающим является Закон Республики Беларусь «Об информации, информатизации и защите информации», который определяет цели, основные требования и меры защиты (правовые организационные, технические), права и обязанности субъектов информационных отношений по защите информации. В нем впервые на уровне законодательства определено понятие «защиты информации». Так, под защитой информации понимается комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. Также впервые законодательно закрепляются права и обязанности граждан, организаций и государства в информационной области, устанавливается правовой режим обработки и использования информации, порядок защиты прав субъектов информационных отношений. В указанном Законе формулируются следующие цели защиты информации:

– обеспечение национальной безопасности, суверенитета Республики Беларусь;

– сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в информационных системах;

– обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

– недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Закон впервые в законодательной практике Республики Беларусь нормативно урегулировал следующие вопросы:

– закрепил права граждан, организаций и государства на информацию;

– установил правовой режим информации на основе применения в этой области института собственности, правил документирования, деления информации на открытую и закрытую (с ограниченным доступом), методов формирования информационных ресурсов и пользования ими;

– установил основные права и обязанности граждан, организаций и государства в процессе создания информационных систем, развития научно-технической базы информатизации, формирования рынка информационной продукции и информационных услуг;

– установил гарантии безопасности субъектов в процессе реализации их права на информацию;

– определил порядок включения страны в международные информационные системы

Законом определены правовые, организационные и технические меры по защите информации. К правовым мерам отнесены заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий; к организационным мерам – обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации; к техническим – использование средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

В Гражданском кодексе Республики Беларусь содержатся нормы, касающиеся служебной и коммерческой тайны, закрепляется такая форма отношений, как информационные услуги, электронная подпись признается как средство, подтверждающее подлинность сторон в сделках, предусматривается ответственность за незаконное использование информации.

В Уголовном кодексе Республики Беларусь закрепляется ответственность за преступления против информационной безопасности (гл. 31), а также иные составы преступлений в информационной сфере (хищение путем использования компьютерной техники (ст. 212), умышленное разглашение государственной тайны (ст. 373), разглашение государственной тайны по неосторожности (ст. 374), умышленное разглашение служебной тайны (ст. 375) и т. д.).

Кодексом Республики Беларусь об административных правонарушениях определяются административно-правовые санкции за правонарушения в информационной сфере. К таким правонарушениям относятся: отказ в предоставлении гражданину информации (ст. 9.6), несанкционированный доступ к компьютерной информации (ст. 22.6), нарушение правил защиты информации (ст. 22.7) и т. д.

Правовые нормы активно применяются в республике для пресечения действий, направленных на нарушение информационной безопасности субъектов хозяйствования. Примером может послужить ситуация, сложившаяся в РУП «Белтаможсервис».

В компьютерах, обслуживающих деятельность предприятия, были обнаружены программные закладки. Следственным управлением УСК по г. Минску в мае 2018 года было возбуждено уголовное дело о несанкционированном доступе и копировании информации из базы данных РУП «Белтаможсервис».

Обвиняемыми и подозреваемыми по уголовному делу были признаны должностные лица ряда организаций, входящих в группу компаний «Vim Union», в том числе действующие руководители данных предприятий.

По данным следствия, в период с декабря 2015 по январь 2018 вышеуказанные должностные лица с использованием специально разработанных вредоносных программ осуществляли несанкционированный доступ и копирование информации из базы данных конкурента в сфере таможенного представительства. Указанное программное обеспечение создано бывшим сотрудником РУП «Белтаможсервис», который был осведомлен о существовавшей системе хранения информации на предыдущем месте работы и на протяжении некоторого времени занимал должность специалиста по безопасности в группе компаний «Vim Union».

Действия трех обвиняемых в зависимости от их роли квалифицированы следствием по следующим статьям Уголовного кодекса Республики Беларусь:

ч. 2 ст. 254. Коммерческий шпионаж, повлекший причинение ущерба в особо крупном размере, – наказывается штрафом или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от одного года до пяти лет;

ч. 2 ст. 349. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок;

ст. 352. Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, – наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок;

ч. 2 ст. 354. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами, повлекшие тяжкие последствия, – наказываются лишением свободы на срок от трех до десяти лет.

Подобным способом в распоряжение обвиняемых поступали сведения о поданных электронных таможенных декларациях предприятиями, осуществляющими экспорт и импорт товаров.

Собранная информация использовалась в дальнейшем при осуществлении финансово-хозяйственной деятельности субъектами хозяйствования ООО «МонолитПромИнвест», ООО «Внешевросервис», ООО «Монолитлогистик». С ее помощью оценивались риски

при осуществлении договорных отношений, устанавливался объем товарооборота предприятий, и, что самое важное, проводилась работа по переманиванию крупных клиентов. Имея необходимые сведения, составляющие коммерческую тайну, представители группы компаний «Vim Union» совершали звонки представителям предприятий из базы данных и предлагали свои услуги на более выгодных условиях.

Важную роль в правовом регулировании в области обеспечения информационной безопасности играют указы Президента Республики Беларусь и постановления Совета Министров Республики Беларусь. К таким законодательным актам можно отнести: указы Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь», от 01 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь», от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»; постановления Совета Министров Республики Беларусь от 29 апреля 2010 г. № 64 «О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 19», от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность"» (ТР 2013/027/BY).

Особую часть нормативно-правового обеспечения информационной безопасности составляют технические нормативные правовые акты – стандарты и предстандарты. Первая группа стандартов – стандарты серии 34.101 (Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий). Стандарты устанавливают общие подходы к формированию требований и оценке безопасности информационных технологий, определяют виды требований безопасности и содержат их систематизированный каталог, критерии и уровни оценки безопасности информационных технологий, позволяющие оценить правильность

реализации средств безопасности, стойкость механизмов защиты. В целом, разработка указанных стандартов осуществляется посредством принятия и использования международных стандартов в качестве национальных. Достоинства подхода – использование лучших мировых практик, повышение доверия при сертификации продуктов и систем, взаимное признание сертификатов. Недостатки – необходимость проведения идентификации текстов, непрерывного отслеживания и внедрения международной нормативной базы, отставание в принятии и использовании стандартов на 3–5 лет, отсутствие собственных методических и инструментальных средств использования отечественной нормативной базы. Вторая группа представлена стандартами по криптографической защите информации – СТБ 1176.1–99 «Информационная технология. Защита информации. Функция хэширования», СТБ 1176.2–99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи», – применяемыми при разработке средств криптографической защиты и гарантирующими криптостойкость ЭЦП.

Вопросы для самоконтроля

1. Основные задачи правового обеспечения информационной безопасности.
2. Законодательная база по обеспечению информационной безопасности государства и личности.

4. ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – это информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа (*НСД*) – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим НСД к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Информационная безопасность – это защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной – это:

- попытки проникновения злоумышленников;
- ошибки персонала;
- выход из строя аппаратных и программных средств;
- стихийные бедствия (землетрясение, ураган, пожар) и т. п.

Современная **автоматизированная система (АС) обработки информации** представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты АС можно разбить на следующие группы:

– аппаратные средства – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);

– программное обеспечение – приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

– данные – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;

– персонал – обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в АС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, соответствуют физические представления в компьютерной среде:

– для представления информации – машинные носители информации в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;

– объектам системы – пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;

– субъектам системы – активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Основными составляющими информационной безопасности являются конфиденциальность, доступность, целостность.

Конфиденциальность – защита от несанкционированного доступа к информации или гарантия того, что информация будет доступна только тем субъектам, которым разрешен доступ (такие пользователи называются авторизованными).

Доступность – возможность за приемлемое время получить требуемую информационную услугу или гарантия того, что авторизованные пользователи всегда получат доступ к хранящейся в компьютерной системе информации (в любое время, по первому требованию).

Целостность – защищенность информации от разрушения и несанкционированного изменения или гарантия сохранения данными правильных значений, которая обеспечивается запретом их модификации для неавторизованных пользователей.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации – это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ к информации – нарушение установленных правил разграничения доступа. Лицо или процесс, осуществляющие НСД к информации, являются нарушителями правил разграничения доступа. НСД является наиболее распространенным видом компьютерных нарушений.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация. С каждым субъектом системы (сети) связывают некоторую информацию (число, строку символов), идентифицирующую субъект. Эта информация является идентификатором субъекта системы

(сети). Субъект, имеющий зарегистрированный идентификатор, является законным (легальным) субъектом.

Идентификация субъекта – это процедура распознания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть). Следующим шагом взаимодействия системы с субъектом является аутентификация субъекта.

Аутентификация субъекта – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил. После идентификации и аутентификации субъекта выполняют процедуру авторизации.

Авторизация субъекта – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Угрозы информационной безопасности и их классификация

Чтобы выбрать наиболее экономичные средства обеспечения безопасности, необходимо знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют.

Угроза – целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой информации и приводит к ее случайному или предумышленному изменению или уничтожению, то есть под угрозой безопасности информации (информационной угрозой) понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства. Если ценность информации теряется при ее хранении и/или распространении, то реализуется угроза нарушения конфиденциальности информации. Если информация изменяется или уничтожается с потерей ее ценности, то реализуется угроза целостности информации. Если информация вовремя не поступает легальному пользователю, то ценность ее уменьшается и со временем полностью обесценивается, тем самым также реализуется угроза оперативности использования или доступности информации.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (например, ошибок в ПО).

Атака – реализованная угроза безопасности, то есть атакой на компьютерную систему (КС) называют действие, которое заключается в поиске и использовании той или иной уязвимости системы.

Риск – вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.

Чем более уязвимой является существующая система безопасности, тем выше вероятность реализации атаки и, следовательно, тем выше значение риска.

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности.

Пока существует окно опасности, возможны успешные атаки на ИС. Для большинства уязвимых мест окно опасности существует сравнительно долго (дни, недели). За это время должны быть выпущены и затем установлены соответствующие заплаты.

Классификация возможных угроз информационной безопасности АС может быть проведена по следующим базовым признакам:

1. По природе возникновения:

– естественные угрозы, вызванные воздействиями на АС объективных физических процессов или стихийных природных явлений;

– искусственные угрозы безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления:

– угрозы, вызванные ошибками или халатностью персонала (например, некомпетентное использование средств защиты, ввод ошибочных данных и т. п.);

– угрозы преднамеренного действия (например, действия злоумышленников).

3. По непосредственному источнику угроз:

– природная среда (например, стихийные бедствия, магнитные бури и пр.);

– человек (например, вербовка путем подкупа персонала, разглашение конфиденциальных данных и т. п.);

– санкционированные программно-аппаратные средства (например, удаление данных, отказ в работе ОС);

– несанкционированные программно-аппаратные средства (например, заражение компьютера вирусами с деструктивными функциями).

4. По положению источника угроз:

– вне контролируемой зоны АС (например, перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств);

– в пределах контролируемой зоны АС (например, применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т. п.);

– непосредственно в АС (например, некорректное использование ресурсов АС).

5. По степени зависимости от активности АС:

– независимо от активности АС (например, вскрытие шифров криптозащиты информации);

– только в процессе обработки данных (например, угрозы выполнения и распространения программных вирусов).

6. По степени воздействия на АС:

– пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (например, угроза копирования секретных данных);

– активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС (например, внедрение троянских коней и вирусов).

7. По этапам доступа пользователей или программ к ресурсам АС:

– угрозы, появляющиеся на этапе доступа к ресурсам АС (например, угрозы несанкционированного доступа в АС);

– угрозы, появляющиеся после разрешения доступа к ресурсам АС (например, угрозы несанкционированного или некорректного использования ресурсов АС).

8. По способу доступа к ресурсам АС:

– угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам АС (например, незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя);

– угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам АС (например, несанкционированный доступ к ресурсам АС путем использования недокументированных возможностей ОС).

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС:

– угрозы доступа к информации, находящейся на внешних запоминающих устройствах (например, несанкционированное копирование секретной информации с жесткого диска);

– угрозы доступа к информации, находящейся в оперативной памяти (например, чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ);

– угрозы доступа к информации, циркулирующей в линиях связи (например, незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений);

– угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (например, запись отображаемой информации на скрытую видеокамеру).

Рассмотрим функции компьютерной системы как объекта, предоставляющего информацию.

В общем случае мы имеем дело с потоком информации от некоторого источника, например файла или области памяти, к адресату, например в файл или к пользователю.

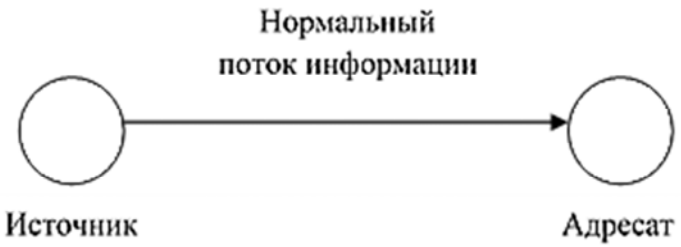

Рис. 1

Существует 4 типа атак (нарушений нормального потока информации):

1. Разъединение. Ресурс уничтожается, становится недоступным либо непригодным к использованию. При этом нарушается доступность информации.

Примеры: вывод из строя оборудования (порча винчестера), обрыв линий связи, удаление файла и т. д.

2. Перехват. К ресурсу открывается несанкционированный доступ. Нарушается конфиденциальность информации. Получившим несанкционированный доступ нарушителем может быть физическое лицо, ПО, компьютер.

Пример: подключение к сетевому кабелю с целью перехвата данных и незаконное копирование файлов и программ.

3. Модификация. К ресурсу не только открывается несанкционированный доступ, но нарушитель еще и изменяет ресурс. Нарушается целостность информации.

Примеры: изменение значений в файле данных, модификация программы с целью изменения ее функций и характеристик, изменение содержимого передаваемого сообщения.

4. Фальсификация. В систему злоумышленником вносится подложный объект. Нарушается аутентичность информации (аутентификация – подтверждение подлинности).

Пример: отправка поддельных сообщений по сети.

Наиболее распространенные угрозы безопасности. Каналы утечки информации

Искусственные угрозы, исходя из их мотивов, разделяются на непреднамеренные (случайные) и преднамеренные (умышленные).

К **непреднамеренным угрозам** относятся:

– ошибки в проектировании компьютерных систем (КС);

– ошибки в разработке программных средств КС;

– случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;

– ошибки пользователей КС;

– воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

К **умышленным угрозам** относятся:

– несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

– несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

В зависимости от целей преднамеренных угроз безопасности информации в КС угрозы могут быть разделены на три основные группы:

– угроза нарушения конфиденциальности, то есть утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

– угроза нарушения целостности, то есть преднамеренного воздействия на информацию, хранящуюся в КС или передаваемую между КС (целостность информации также может быть нарушена, если к несанкционированному изменению или уничтожению информации приводит случайная ошибка в работе программных или аппаратных средств КС; санкционированным является изменение или уничтожение информации, сделанное уполномоченным лицом с обоснованной целью);

– угроза нарушения доступности информации, то есть отказа в обслуживании, вызванного преднамеренными действиями одного из пользователей КС (нарушителя), при котором блокируется доступ к некоторому ресурсу КС со стороны других пользователей КС (постоянно или на большой период времени).

Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.

Результатом реализации угроз безопасности информации в КС может быть утечка (копирование) информации, ее утрата (разрушение) или искажение (подделка), блокирование информации.

Возможные **каналы утечки информации** можно классифицировать следующим образом:

1. Косвенные каналы утечки – это каналы, не связанные с физическим доступом к элементам КС. К ним относятся:

– использование подслушивающих (радиозакладных) устройств;

– дистанционное наблюдение;

– перехват побочных электромагнитных излучений и наводок (ПЭМИН).

2. Непосредственные каналы, связанные с физическим доступом к элементам КС.

К непосредственным каналам утечки, не требующим изменения элементов КС, относятся:

– хищение носителей информации;

– сбор производственных отходов с информацией (бумажных и магнитных носителей);

– намеренное копирование файлов других пользователей КС;

– чтение остаточной информации после выполнения заданий других пользователей (областей оперативной памяти, удаленных файлов, ошибочно сохраненных временных файлов);

– копирование носителей информации;

– намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей КС;

– маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т. п.);

– обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.

К непосредственным каналам утечки, предполагающим изменение элементов КС и ее структуры, относятся:

– незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи (пассивное для фиксации и сохранения передаваемых данных или активное для их уничтожения, искажения или подмены);

– злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

– злоумышленный вывод из строя средств защиты информации.

Поскольку наиболее опасные угрозы информационной безопасности вызваны преднамеренными действиями нарушителя, которые в общем случае являются неформальными, проблема защиты информации относится к формально не определенным проблемам. Отсюда следует два основных вывода:

1) надежная защита информации в КС не может быть обеспечена только формальными методами (например, только программными и аппаратными средствами);

2) защита информации в КС не может быть абсолютной.

При решении задачи защиты информации необходимо применять системно-концептуальный подход, в соответствии с которым решение задачи должно подразумевать:

– *системность целевую*, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества;

– *системность пространственную*, предполагающую взаимосвязанность защиты информации во всех элементах КС;

– *системность временную*, предполагающую непрерывность защиты информации;

– *системность организационную*, предполагающую единство организации всех работ по защите информации в КС и управления ими.

Обеспечение информационной безопасности КС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Существующие методы и средства защиты информации можно подразделить на четыре основные группы:

1) методы и средства организационно-правовой защиты информации;

2) методы и средства инженерно-технической защиты информации;

3) криптографические методы и средства защиты информации;

4) программно-аппаратные методы и средства защиты информации.

Вопросы для самоконтроля

1. В чем суть понятия «защита информации»?
2. Что является объектом защиты информации и каковы цели защиты информации?
3. Назовите основные составляющие информационной безопасности и дайте им краткую характеристику.
4. Что в себя включает система защиты информации?
5. Объясните суть понятий санкционированный доступ к информации и несанкционированный доступ к информации.
6. Что такое идентификация, аутентификация и авторизация субъекта системы (сети)?
7. Раскройте суть таких понятий информационной безопасности, как угроза, атака, риск.
8. Как классифицируются возможные угрозы информационной безопасности АС?
9. Какие существуют типы атак на информационную систему (или нарушений нормального потока информации)?
10. Назовите возможные каналы утечки информации.

5. ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Основными способами несанкционированного доступа к информации в КС являются:

– непосредственное обращение к объекту с конфиденциальной информацией (например, с помощью управляемой пользователем программы, читающей данные из файла или записывающей их в нее);

– создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты (например, с использованием случайно или намеренно оставленных разработчиком этих средств, так называемых люков);

– модификация средств защиты для осуществления несанкционированного доступа (например, внедрение программных закладок);

– внедрение в технические средства СВТ (средств вычислительной техники) или АС (автоматизированных систем) программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа (например, путем загрузки на компьютере иной, незащищенной операционной системы).

Модель нарушителя определяется исходя из следующих предположений:

– нарушитель имеет доступ к работе со штатными средствами КС;

– нарушитель является специалистом высшей квалификации, то есть знает все о КС и, в частности, о системе и средствах ее защиты.

Выделяют следующие уровни возможностей нарушителя, предоставляемые ему штатными средствами КС (каждый следующий уровень включает в себя предыдущий):

1) запуск программ из фиксированного набора (например, подготовка документов или получение почтовых сообщений);

2) создание и запуск собственных программ (возможности опытного пользователя или пользователя с полномочиями отладки программ);

3) управление функционированием КС – воздействие на ее базовое программное обеспечение, состав и конфигурацию КС (например, внедрение программной закладки);

4) весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт средств КС, вплоть до включения в состав КС собственных СВТ с новыми функциями.

С учетом различных уровней возможностей нарушителя выделяют следующие вспомогательные способы несанкционированного доступа к информации в КС, позволяющие нарушителю использовать перечисленные ранее основные способы:

– ручной или программный подбор паролей путем их полного перебора или при помощи специального словаря (взлом КС);

– подключение к КС в момент кратковременного прекращения работы легального пользователя, работающего в интерактивном режиме и не заблокировавшего свой терминал;

– подключение к линии связи и перехват доступа к КС после отправки пакета завершения сеанса легального пользователя, работающего в удаленном режиме;

– выдача себя за легального пользователя с применением похищенной у него или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации – «маскарад»;

– создание условий для связи по компьютерной сети легального пользователя с терминалом нарушителя, выдающего себя за легального объекта КС (например, одного из его серверов), – «мистификация»;

– создание условий для возникновения в работе КС сбоев, которые могут повлечь за собой отключение средств защиты информации или нарушение правил политики безопасности;

– тщательное изучение подсистемы защиты КС и используемой в ней политики безопасности, выявление ошибочных участков в программных средствах защиты информации в КС, введение программных закладок, разрешающих доступ нарушителю.

Методы защиты от НСД в компьютерных системах

Основными направлениями обеспечения защиты СВТ и АС от несанкционированного доступа являются создание **системы разграничения доступа** (СРД) субъектов к объектам доступа и создание обеспечивающих средств для СРД.

К основным функциям системы разграничения доступа (СРД) относятся:

– реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания ее твердых копий;

– изоляция процессов, выполняемых в интересах субъекта доступа, от других субъектов;

– управление потоками информации в целях предотвращения ее записи на носители несоответствующего уровня конфиденциальности;

– реализация правил обмена информацией между субъектами в компьютерных сетях.

К функциям обеспечивающих средств для СРД относятся:

– идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для него;

– регистрация действий субъекта и активизированного им процесса;

– исключение и включение новых субъектов и объектов доступа, изменение полномочий субъектов;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка, восстановление объекта после несанкционированного доступа);

– учет выходных печатных форм в КС;

– контроль целостности программной и информационной части СРД и обеспечивающих ее средств.

Таким образом, основными способами защиты от несанкционированного доступа к информации в компьютерных системах являются:

– аутентификация;

– авторизация (определение прав доступа субъекта к объекту с конфиденциальной информацией);

– шифрование информации.

Идентификация (Identification) – процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Под **протоколом** в общем случае понимают конечную последовательность однозначно и точно определенных действий, выполняемых двумя или более сторонами для достижения желаемого результата за конечное время.

Протокол идентификации пользователя при его входе в КС следующий:

1. **Система:** запрос имени, под которым пользователь зарегистрирован в базе данных учетных записей КС (логического имени пользователя, или логина).
2. **Пользователь:** ввод логического имени (ID).
3. **Система:** проверка наличия ID в регистрационной базе данных. Если пользователь с таким именем зарегистрирован, то запрос его идентифицирующей информации, в противном случае – возврат к **пункту 1**.
4. **Пользователь:** ввод идентифицирующей информации (P).
5. **Система:** проверка совпадения P с идентифицирующей информацией для пользователя ID в регистрационной базе данных. Если совпадение есть, то допуск пользователя к работе в КС, в противном случае – возврат к **пункту 3**.

Присвоение каждому пользователю КС уникального логического имени, под которым он регистрируется в базе данных учетных записей, не только позволяет предоставить разным пользователям КС различный уровень прав в ней, но и дает возможность полного учета всех входов пользователя в систему в журнале аудита.

Доступ же к базе данных учетных записей КС как по чтению, так и по записи должен быть разрешен только привилегированному пользователю (то есть администратору).

Аутентификация (Authentication) – процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. Пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Способы аутентификации пользователя в КС можно подразделить на три группы:

1. Способы аутентификации, основанные на том, что пользователь знает некоторую подтверждающую его подлинность информа-

цию (парольная аутентификация и аутентификация на основе модели «рукопожатия»).

2. Способы аутентификации, основанные на том, что пользователь имеет некоторый материальный объект, который может подтвердить его подлинность (например, пластиковую карту с идентифицирующей пользователя информацией).

3. Способы аутентификации, основанные на таких данных, которые позволяют однозначно считать, что пользователь есть тот самый субъект, за которого себя выдает (биометрические данные, особенности клавиатурного почерка и росписи мышью и т. п.).

Аутентификация пользователей на основе паролей и модели «рукопожатия»

При выборе паролей пользователи КС должны руководствоваться двумя правилами: пароли должны трудно подбираться и легко запоминаться (поскольку пароль ни при каких условиях не должен нигде записываться, так как в этом случае необходимо будет дополнительно решать задачу защиты носителя пароля).

Сложность выбираемых пользователями КС паролей должна устанавливаться администратором при реализации установленной системы политики безопасности. Другими параметрами политики учетных записей при использовании парольной аутентификации должны быть:

- максимальный срок действия пароля;
- несовпадение пароля с логическим именем пользователя, под которым он зарегистрирован в КС;
- неповторяемость паролей одного пользователя.

Аутентификация на основе многоразовых паролей

В современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных (БД). В этой БД хранятся учетные данные о пользователях сети, включающие идентификаторы и пароли пользователей, а также другую информацию.

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. Пользователь при попытке логического входа в сеть набирает свой идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В БД, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись. Из нее извлекается пароль и сравнивается с тем паролем, который ввел пользователь. Если они совпали, то аутентификация прошла успешно – пользователь получает легальный статус и получает те права и ресурсы сети, которые определены для его статуса системой авторизации.

В схеме простой аутентификации передача пароля и идентификатора пользователя может производиться следующими способами:

1) в незашифрованном виде, например, согласно протоколу парольной аутентификации PAP (Password Authentication Protocol) пароли передаются по линии связи в открытой незащищенной форме;

2) в защищенном виде. Все передаваемые данные (идентификатор и пароль пользователя, случайное число и метки времени) защищены посредством шифрования или однонаправленной функции.

Системы простой аутентификации на основе многоразовых паролей имеют пониженную стойкость, поскольку выбор аутентифицирующей информации происходит из относительно небольшого числа слов. Срок действия многоразового пароля должен быть определен в политике безопасности организации. Пароли должны регулярно изменяться, быть трудными для угадывания и не присутствовать в словаре.

Аутентификация на основе одноразовых паролей

Суть схемы одноразовых паролей – использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, затем его действие истекает. Даже если его перехватили, он будет бесполезен.

Динамический механизм задания пароля – один из лучших способов защиты процесса аутентификации от угроз извне. Обычно система аутентификации с одноразовым паролем используется для проверки удаленных пользователей.

Генерация одноразовых паролей может осуществляться аппаратным и программным способом. Некоторые аппаратные средства доступа на основе одноразовых паролей реализуются в виде миниатюрных устройств со встроенным микропроцессором, внешне похожих на платежные пластиковые карточки. Такие карты, называемые ключами, могут иметь клавиатуру и небольшое дисплейное окно.

Аутентификация на основе модели «рукопожатия»

Для организации аутентификации при удаленном взаимодействии используется стандартный протокол CHAP (Challenge Handshake Authentication Protocol), или как его называют – «по рукопожатию».

В этом протоколе используется секретный статический пароль. Такой пароль каждого пользователя для передачи по линии связи шифруется на основе случайного числа, полученного от сервера. Такая технология обеспечивает не только защиту пароля от хищения, но и защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем. Шифрование пароля в соответствии с протоколом CHAP выполняется с помощью криптографического алгоритма хэширования и поэтому является необратимым. Функция хэширования (хэш-функция) представляет собой преобразование, на вход которого подается сообщение переменной длины, а выходом является строка фиксированной длины. В стандарте для протокола CHAP в качестве хэш-функции определен алгоритм MD, вырабатывающий из входной последовательности любой длины 16-байтовое значение (хотя минимальной длиной секрета является 1 байт, для повышения криптостойкости рекомендуется использовать секрет длиной не менее 16 байт).

Аутентификация пользователей на основе PIN-кода

Наиболее распространенным методом аутентификации держателя пластиковой карты и смарт-карты является ввод секретного числа, которое называют PIN-кодом (Personal Identification Number – персональный идентификационный код). Защита PIN-кода карты является критичной для безопасности всей системы.

Согласно рекомендации стандарта ISO 9564-1, PIN-код должен содержать от 4 до 12 буквенно-цифровых символов. Однако в большинстве случаев ввод нецифровых символов технически невозможен, так как доступна только цифровая клавиатура. Обычно PIN-код представляет собой четырехразрядное число, каждая цифра которого может принимать значение от 0 до 9.

PIN-код вводится с помощью клавиатуры терминала или компьютера и затем отправляется на смарт-карту. Смарт-карта сравнивает полученное значение PIN-кода с эталонным значением, хранимым в карте, и отправляет результат сравнения на терминал. Ввод PIN-кода относится к мерам безопасности, поэтому PIN-клавиатуры имеют все признаки модуля безопасности и шифруют PIN-код сразу при его вводе. Это обеспечивает надежную защиту от проникновения в клавиатуру для перехвата PIN-кода во время ввода.

Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью

К основным биометрическим характеристикам пользователей КС, которые могут применяться при их аутентификации, относятся:

- отпечатки пальцев;
- геометрическая форма кисти руки;
- узор радужной оболочки глаза;
- рисунок сетчатки глаза;
- геометрическая форма и размеры лица;
- тембр голоса;
- геометрическая форма и размеры уха и др.

Наиболее распространенными являются программно-аппаратные средства аутентификации пользователей по их отпечаткам пальцев. Для считывания этих отпечатков применяются оснащенные специальными сканерами клавиатуры и мыши. Наличие достаточно больших банков данных с отпечатками пальцев граждан является основной причиной достаточно широкого применения подобных средств аутентификации в государственных структурах, а также в крупных коммерческих организациях.

Если по объективным причинам (например, из-за загрязненности помещений, в которых проводится аутентификация) получение четкого отпечатка пальца невозможно, то может применяться аутентификация по геометрической форме руки пользователя. В этом случае сканеры могут быть установлены на стене помещения.

Наиболее достоверными (но и более дорогостоящими) являются средства аутентификации пользователей, основанные на характеристиках глаза (узоре радужной оболочки или рисунке сетчатки). Вероятность повторения этих признаков оценивается в 10^{-78}.

Наиболее дешевыми (но и наименее достоверными) являются средства аутентификации, основанные на геометрической форме и размере лица пользователя или на тембре его голоса.

Способы аутентификации, основанные на особенностях клавиатурного почерка и росписи мышью пользователей, не требуют применения специальной аппаратуры.

Сутью способа аутентификации на основе клавиатурного почерка является проверка гипотезы о равенстве центров распределения двух нормальных генеральных совокупностей (полученных при настройке системы на такие характеристики регистрируемого пользователя и при его аутентификации, как: выбор пользователем ключевой фразы; набор ключевой фразы несколько раз; исключение грубых ошибок и т. п.).

Достоверность аутентификации на основе клавиатурного почерка или росписи мышью пользователя намного ниже, чем при использовании его биометрических характеристик, так как особенностью этих способов аутентификации является нестабильность их характеристик у одного и того же пользователя, которая может быть вызвана:

1) естественными изменениями, связанными с улучшением (или ухудшением) навыков пользования по работе с клавиатурой и мышью;

2) изменениями, связанными с ненормальным физическим или эмоциональным состоянием пользователя.

Программно-аппаратная защита информации от локального несанкционированного доступа

Недостатки парольной аутентификации пользователей КС могут быть устранены применением двухфакторной аутентификации, при которой пользователь для входа в систему должен не только ввести

пароль, но и предъявить элемент аппаратного обеспечения, содержащий подтверждающую его подлинность ключевую информацию. Такими элементами аппаратного обеспечения могут быть:

– магнитные диски, не требующие установки на компьютере пользователя КС никаких дополнительных аппаратных средств, но наиболее уязвимые с точки зрения копирования хранящейся на них информации;

– элементы Touch Memory, включающие в себя энергозависимую память в виде постоянного запоминающего устройства (ПЗУ) с уникальным для каждого изделия серийным номером и оперативного запоминающего устройства (ПЗУ) для хранения идентифицирующей пользователя информации, а также встроенный элемент питания со сроком службы до 10 лет (элемент Touch Memory напоминает миниатюрную батарейку диаметром 16 мм и толщиной 3–6 мм, он имеет один сигнальный контакт и один контакт заземления, а для контакта элемента с устройством чтения достаточно простого касания);

– пластиковые карты с магнитной полосой, на которой помимо ключевой информации могут размещаться и дополнительные реквизиты пользователя: его фамилия, имя, отчество, фотография, название организации и т. п. (подобные карты наиболее дешевые, но и наименее защищенные от копирования и подделки);

– карты со штрихкодом, покрытым непрозрачным составом, считывание информации с которых происходит в инфракрасных лучах (эти карты относительно дешевые, но они уязвимы для подделки);

– смарт-карты, носителем ключевой информации в которых является специальная бескорпусная микросхема, включающая в себя только память для хранения ключевой информации (простые смарт-карты) или микропроцессор (интеллектуальные карты), позволяющие реализовывать достаточно сложные процедуры аутентификации;

– маркеры eToken (USB-брелки), представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную смарт-карте микросхему с процессором и защищенной от несанкционированного доступа памятью (в отличие от пластиковых карт не требует установки устройства их чтения с кабелем для подключения этого устройства к компьютеру).

Программные средства системы защиты информации должны быть записаны на плате расширения BIOS, для каждой из которых

определен уникальный пароль установки. Установка системы защиты информации производится на компьютере, свободном от вредоносных программ типа закладок и вирусов.

После установки платы расширения BIOS выполняется процедура установки системы защиты информации:

1) после включения питания компьютера программа, записанная на плате расширения BIOS, выдает запрос на ввод пароля;

2) после ввода пароля установки (как правило, администратором системы) происходит загрузка операционной системы и запуск программы установки (проверочные функции системы защиты при этом отключаются);

3) по запросу программы установки вводится пароль пользователя, ключевая информация с элемента аппаратного обеспечения (например, серийный номер элемента Touch Memory) и имена подлежащих проверке системных и пользовательских файлов;

4) для каждого указанного файла вычисляется и сохраняется проверочная информация.

Процедура входа пользователя в КС при использовании программно-аппаратной системы защиты от НСД следующая:

1) после включения питания компьютера программа на плате расширения BIOS запрашивает пароль пользователя и просит установить элемент аппаратного обеспечения с его ключевой информацией;

2) осуществляется проверка целостности выбранных при установке системы защиты файлов;

3) в зависимости от результатов проверки выполняется либо загрузка операционной системы, либо запрос на повторный ввод пароля.

После завершения работы пользователя элемент аппаратного обеспечения с его ключевой информацией изымается из компьютера.

Вопросы для самоконтроля

1. Какие существуют основные способы несанкционированного доступа к информации в КС?
2. Чем характеризуется модель нарушителя информационной безопасности КС?
3. Какие существуют вспомогательные способы несанкционированного доступа к информации в КС?

4. Что собой представляет система разграничения доступа (СРД) и каковы ее функции?

5. В чем суть процедуры *идентификации* пользователя и каков протокол идентификации пользователя при его входе в КС?

6. В чем суть процедуры *аутентификации* пользователя и на какие группы подразделяются способы аутентификации пользователя в КС?

7. Как выполняются процедуры аутентификации на основе многоразовых и одноразовых паролей?

8. Как выполняется процедура аутентификации на основе модели «рукопожатия»?

9. Как выполняется процедура аутентификации пользователей на основе PIN-кода?

10. Как выполняются процедуры аутентификации пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью?

11. Какие существуют способы программно-аппаратной защиты информации от локального несанкционированного доступа?

6. БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННОЙ СРЕДЫ

Функции и назначение межсетевых экранов

Межсетевой экран (**МЭ**) (или **сетевой экран**) – это специализированный комплекс аппаратной или программной межсетевой защиты, называемый также **брандмауэром** или системой **firewall**, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

– *традиционный сетевой (или межсетевой) экран* – программа (или неотъемлемая часть операционной системы) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями.

– *персональный сетевой экран* – программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

МЭ еще можно представить как набор фильтров, пропускающих через себя весь трафик, анализирующих проходящую через них информацию и принимающих решение: пропустить информацию или ее заблокировать. Одновременно с этим производится регистрация событий и тревожная сигнализация в случае обнаружения угрозы.

МЭ позволяет разделить общую сеть на две части (или более) и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Такая граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet.

МЭ, защищающий сразу множество узлов внутренней сети, призван решить:

1) задачу ограничения доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых МЭ;

2) задачу разграничения доступа пользователей защищаемой сети к внешним ресурсам. Это позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей.

Функции МЭ следующие:

1. **Фильтрация трафика**. Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации, которые могут задавать: блокирование потока данных; обработку данных от имени получателя и возврат результата отправителю; передачу данных на следующий фильтр для продолжения анализа; пропускание данных, игнорируя следующие фильтры; дополнительные действия (например, преобразование данных, регистрация событий и т. д.).

2. **Выполнение функций посредничества**. Эти функции МЭ выполняет с помощью специальных программ, называемых экранирующими агентами или программами-посредниками, которые являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью. При необходимости доступа из внутренней сети во внешнюю или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений и осуществлять другие защитные функции.

3. **Дополнительные функции:**

а) *идентификация* и *аутентификация* пользователей, с помощью которых осуществляется разрешение или запрещение допуска различных приложений и пользователей в сеть;

б) *трансляция сетевых адресов*, которая выполняется для того, чтобы скрыть внутренние сетевые адреса, а также топологию всей сети от атак злоумышленника. Трансляция внутренних сетевых адресов может осуществляться двумя способами – динамически и ста-

тически. В случае динамической, адрес выделяется узлу в момент обращения к МЭ и после завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. В случае статистической, адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. При этом IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внутренней сетью;

в) *администрирование*, которое является одним из ключевых аспектов в создании надежной и эффективной системы защиты. Ошибки при определении правил доступа могут образовывать дыру, через которую возможен взлом системы. Поэтому в большинстве МЭ реализованы сервисные утилиты, позволяющие просматривать информацию, сгруппированную по каким-либо критериям, например все, что относится к конкретному пользователю;

г) *регистрация событий* и *генерация отчетов*. МЭ регистрирует такие действия, как пропуск или блокирование сетевых пакетов, изменение правил разграничения доступа администратором безопасности и другие действия. МЭ позволяют произвести анализ такой статистики и предоставить администратору подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об попытках выполнения несанкционированных действий.

Виртуальные частные сети (VPN), их назначение и использование в информационных системах

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 1990-х гг. родилась и активно развивается концепция построения **виртуальных частных сетей – VPN** (Virtual Private Network).

Виртуальной защищенной сетью (VPN) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих дан-

ных, то есть *виртуальная частная сеть* – технология безопасного подключения к корпоративной сети через Интернет. Данная технология является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

– *шифрования* (с использованием инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);

– *экранирования* (с использованием межсетевых экранов);

– *туннелирования*.

Сущность технологии VPN заключается в следующем (рис. 2):

1. На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливаются VPN-агенты (программные или программно-аппаратные комплексы, выполняемые на базе персональных компьютеров или компьютеров, выполняющих роль серверов), которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

2. Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

– анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

– вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;

– пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

– формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для

внешней атаки информация, например внутренние IP-адреса сети, в этом случае недоступна.

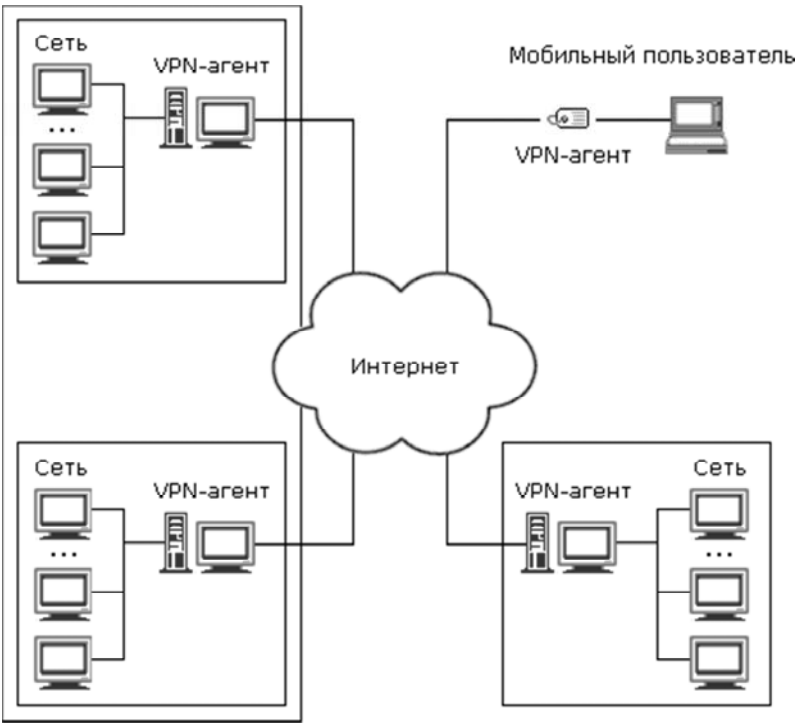

Рис. 2

3. При получении IP-пакета выполняются обратные действия:

– из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);

– согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

– после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется **туннелем**, а технология его создания называется «туннелированием»). Вся информация передается по туннелю в зашифрованном виде.

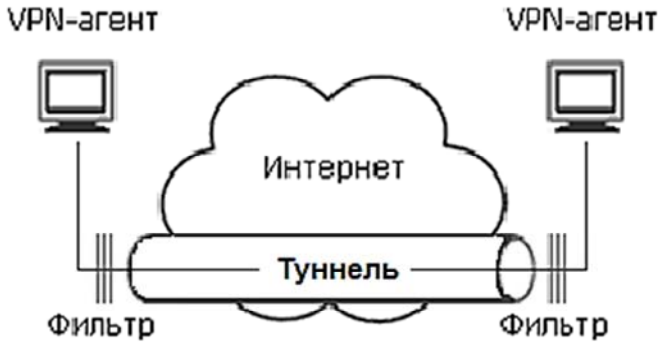

Рис. 3

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

Достоинства использования VPN-технологий для защиты информации в распределенных сетевых ИС масштаба предприятия следующие:

1) возможность защиты всей корпоративной сети – от крупных локальных сетей офисов до отдельных рабочих мест. Защита может

быть распространена на все звенья сети – от сегментов локальных сетей до коммуникационных каналов глобальных сетей, в том числе выделенных и коммутируемых линий;

2) масштабируемость системы защиты, то есть для защиты объектов различной сложности и производительности можно использовать адекватные по уровню сложности, производительности и стоимости программные или программно-аппаратные средства защиты;

3) использование ресурсов открытых сетей в качестве отдельных коммуникационных звеньев корпоративной сети. Все угрозы, возникающие при использовании сетей общего пользования, будут компенсироваться средствами защиты информации;

4) обеспечение подконтрольности работы сети и достоверная идентификация всех источников информации. При необходимости может быть обеспечена аутентификация трафика на уровне отдельных пользователей;

5) сегментация ИС и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.

Вопросы для самоконтроля

1. Каково назначение межсетевых экранов, как они классифицируются, какие задачи защиты узлов внутренней сети решают?
2. Перечислите основные и дополнительные функции межсетевых экранов.
3. Что такое виртуальная частная сеть (VPN) и какие сервисы (механизмы) безопасности в нее входят?
4. Поясните сущность технологии виртуальных частных сетей (VPN).
5. Каковы достоинства использования VPN-технологий для защиты информации в распределенных сетевых ИС масштаба предприятия?

7. ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

Вредоносная программа – это программа, наносящая какой-либо вред компьютеру, на котором она запускается, или другим компьютерам в сети.

К вредоносным программам относятся компьютерные вирусы и программные закладки.

Компьютерным вирусом называют автономно функционирующую программу, обладающую следующими свойствами:

– способностью к включению своего кода в тела других файлов и системных областей памяти компьютера;

– последующему самостоятельному выполнению;

– самостоятельному распространению в компьютерных системах.

Программной закладкой называют внешнюю или внутреннюю по отношению к атакуемой компьютерной системе программу, обладающую определенными разрушительными функциями по отношению к этой системе:

– уничтожение или внесение изменений в функционирование программного обеспечения КС, уничтожение или изменение обрабатываемых в ней данных после выполнения некоторого условия или получения некоторого сообщения извне КС («логические бомбы»);

– превышение полномочий пользователя с целью несанкционированного копирования конфиденциальной информации других пользователей КС или создания условий для такого копирования («троянские» программы);

– подмена отдельных функций подсистемы защиты КС или создание люков в ней для реализации угроз безопасности информации в КС (например, подмена средств шифрования путем эмуляции работы установленной в КС платы аппаратного шифрования);

– перехват паролей пользователей КС с помощью имитации приглашения к его вводу или перехват всего ввода пользователей с клавиатуры;

– перехват потока информации, передаваемой между объектами распределенной КС (мониторы);

– распространение в распределенных КС с целью реализации той или иной угрозы безопасности информации (компьютерные черви,

которые в отличие от компьютерных вирусов не должны обладать свойством включения своего кода в тела других файлов) и др.

Компьютерные вирусы классифицируются по следующим признакам:

1. По способу распространения в КС:

– *файловые вирусы*, которые заражают файлы одного или нескольких типов: различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов) либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы);

– *загрузочные вирусы* (или *бутовые вирусы*), записывающие себя либо в загрузочный сектор (boot-сектор) диска, либо в сектор, содержащий системный загрузчик винчестера (MasterBootRecord). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносится в какой-либо другой сектор диска;

– *макровирусы*, которые заражают макропрограммы и файлы документов современных систем обработки информации, таких как Word, Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Макровирусы получают управление при открытии зараженного файла и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения;

– *сетевые вирусы*, которые используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа «червь». Сетевые черви подразделяются на Internet-червей (распространяются по Internet), LAN-червей (распространяются по локальной сети), IRC-червей (распространяются через чаты – InternetRelayChat). Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий;

– *комбинированные вирусы*, которые имеют довольно сложный алгоритм работы. Часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии. Например, файлово-загрузочные вирусы, способные заражать и файлы, и загрузочные сектора дисков или сетевые макро-вирусы,

которые не только заражают редактируемые документы, но и рассылают свои копии по электронной почте;

2. По способу заражения других объектов КС:

– *резидентные вирусы*, часть кода которых (то есть их резидентная часть) постоянно находится в оперативной памяти компьютера и заражает другие объекты КС путем перехвата обращения ОС к объектам заражения и внедрения в них. Такие вирусы, находясь в памяти, являются активными вплоть до выключения компьютера или перезагрузки ОС;

– *нерезидентные вирусы*, которые заражают другие объекты КС в момент открытия уже зараженных ими объектов, они не заражают память компьютера и сохраняют активность ограниченное время.

3. По деструктивным возможностям:

– *безвредные вирусы*, в которых реализован только механизм самораспространения, они не наносят вред системе и созданы в целях обучения, однако снижают эффективность работы КС за счет потребления ее ресурсов (времени работы центрального процессора, оперативной и внешней памяти и др.) в результате своего распространения;

– *неопасные вирусы*, присутствие которых в системе связано с различными эффектами (звуковыми или видео) и уменьшением свободной памяти на диске, но которые не наносят вред программам и данным;

– *опасные вирусы*, которые могут привести к серьезным сбоям в работе компьютера, последствием которых может стать разрушение программ и данных;

– *очень опасные вирусы*, в алгоритм работы которых заведомо заложены процедуры, непосредственно приводящие к разрушению программ и данных, стиранию информации, записанной в системных областях памяти и необходимой для работы компьютера, а также нанесению вреда здоровью пользователей (с помощью, например, эффекта двадцать пятого кадра).

4. По особенностям реализуемого алгоритма:

– *вирусы-спутники*, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы (при открытии зараженного файла фактически открывается файл с кодом вируса, в котором после выполнения предусмотренных автором действий открывается исходный файл);

– *паразитические вирусы*, которые обязательно изменяют содержимое зараженных объектов;

– *вирусы-невидимки* (*«стелс»-вирусы*), в которых путем перехвата обращений операционной системы к зараженным объектам и возврата вместо них оригинальных незараженных данных скрывается факт присутствия вируса в КС (при собственном обращении к дисковой памяти вирусы-невидимки также используют нестандартные средства для обхода средств антивирусной защиты);

– *вирусы-призраки* (*самошифрующиеся* или *полиморфные вирусы*), каждая следующая копия которых в зараженных объектах отличается от предыдущих (не содержит одинаковых цепочек команд за счет применения шифрования на различных ключах базового кода вируса).

5. По наличию дополнительных возможностей:

– по обработке атрибута «только чтение» заражаемых файлов;

– сохранению времени последнего изменения зараженного файла;

– обработке прерывания, вызванного неисправимой ошибкой устройства ввода-вывода (например, для подавления сообщения операционной системы об ошибке при попытке заражения объекта на защищенном от записи устройстве или объекта, доступ к которому по записи для текущего пользователя запрещен; вывод подобного сообщения может обнаружить присутствие вируса в КС);

– распространению в КС не только при открытии уже зараженного объекта, но и при выполнении любой операции с ним.

Основные каналы распространения компьютерных вирусов и других вредоносных программ

Основными каналами распространения компьютерных вирусов в настоящее время являются:

– электронная почта, сообщения которой могут содержать зараженные присоединенные файлы;

– телеконференции и электронные доски объявлений в сети Internet;

– свободное и условно свободное программное обеспечение, размещенное на общедоступных узлах сети Internet и случайно или намеренно зараженное вирусами;

– размещенные на общедоступных узлах сети Internet информационные ресурсы, содержащие ссылки на зараженные троянские Web-сайты с элементами управления Active-X или апплетами Java;

– локальные компьютерные сети организаций, создающие удобную среду для заражения вирусами объектов на других рабочих станциях и серверах;

– обмен зараженными файлами на дисках или записываемых компакт-дисках между пользователями сети;

– использование нелицензионных компакт-дисков с программным обеспечением и другими информационными ресурсами.

Методы обнаружения вирусов

К основным методам обнаружения компьютерных вирусов относятся:

1. Метод сравнения с эталоном. Заключается в том, что для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность кода, специфичная для конкретного вируса. Антивирусная программа последовательно просматривает (сканирует) проверяемые файлы в поиске масок известных вирусов. Антивирусные сканеры способны найти только уже известные вирусы, для которых определена маска. Однако для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить маску, поэтому антивирусные сканеры их не обнаруживают.

2. Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен выполнять такие действия, как: копирование в память, запись в секторы и т. д. Эвристический анализатор (который является частью антивирусного ядра) содержит список таких действий и проверяет программы и загрузочные секторы дисков, пытаясь обнаружить в них код, характерный для вирусов. Обнаружив зараженный файл, анализатор выводит сообщение на экране монитора и делает запись в собственном или системном журнале. Эвристический анализ позволяет обнаруживать неизвестные ранее вирусы. Практически все современные антивирусные программы реализуют собственные методы эвристического анализа.

3. Антивирусный мониторинг. Суть метода в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с компакт-диска. Антивирусный мониторинг сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Пример такой программы – сторож SpiderGuard, который входит в комплект сканера DoctorWeb и выполняет функции антивирусного монитора.

4. Метод обнаружения изменений. При реализации этого метода антивирусные программы, называемые ревизорами диска, запоминают предварительно характеристики всех областей диска, которые могут подвергнуться нападению, а затем периодически проверяют их. Заражая компьютер, вирус изменяет содержимое жесткого диска, например дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл Autoexec.bat, изменяет загрузочный сектор, создает файл-спутник. При сопоставлении значений характеристик областей диска антивирусная программа может обнаружить изменения, сделанные как известным, так и неизвестным вирусом.

5. Встраивание антивирусов в BIOS компьютера. В системные платы компьютеров встраивают простейшие средства защиты от вирусов, которые позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам обычных дисков. Если какая-либо программа пытается изменить содержимое загрузочных секторов, срабатывает защита, и пользователь получает соответствующее предупреждение. Но эта защита не очень надежна, так как известны вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергозависимой памяти компьютера (CMOS-памяти).

Антивирусные программы и комплексы

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Однако не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

Различают следующие виды антивирусных программ:

1. Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования вначале в оперативной памяти, а затем в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами области памяти и файлы, но и «лечат» их (то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние). Среди фагов выделяют **полифаги** – программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-фаги делятся на две категории:

1) *универсальные сканеры*, осуществляющие поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер;

2) *специализированные сканеры*, предназначенные для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Программы-фаги также делятся на:

– *резидентные мониторы*, производящие сканирование «на лету» и обеспечивающие более надежную защиту системы, поскольку они немедленно реагируют на появление вируса;

– *нерезидентные сканеры*, обеспечивающие проверку системы только по запросу и способные опознавать вирус только во время своего очередного запуска.

Достоинство программ-фагов всех типов – их универсальность. Недостатки – относительно небольшая скорость поиска вирусов и большие размеры антивирусных баз, которые сканерам приходится хранить и пополнять.

2. Программы-ревизоры (CRC-сканеры) используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (кодов технического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также другая информация (длины файлов,

даты их последней модификации и др.) затем сохраняются в базе данных антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

Достоинство CRC-сканеров – они являются довольно мощным средством против вирусов, так как благодаря использованию алгоритма «анти-стелс» практически 100 % вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Недостаток – они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

3. Программы-блокировщики реализуют метод антивирусного мониторинга и являются резидентными программами, перехватывающими «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и другие, которые характерны для вирусов в моменты их размножения. При попытке какой-либо программы произвести данные действия блокировщик посылает пользователю сообщение и предлагает запретить соответствующее действие.

Достоинства блокировщиков – их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения. Недостатки: блокировщики не лечат файлы и диски; существуют пути обхода их защиты; «назойливость» – например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла.

4. Программы-иммунизаторы. Это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа:

– иммунизаторы, сообщающие о заражении, которые обычно записываются в конец файла и при запуске этого файла каждый раз проверяют его на изменение;

– иммунизаторы, блокирующие заражение каким-либо типом вируса, которые защищают систему от поражения вирусом определенного типа, модифицируя программу или диск таким образом, чтобы это не отражалось на их работе, а вирус при этом воспринимает их зараженными и поэтому не внедряется.

Антивирусные программные комплексы

Существует спектр программных комплексов, предназначенных для профилактики заражения вирусом, обнаружения и уничтожения вирусов. Они обладают универсальностью, гибкостью и адаптивностью.

Наиболее распространенные антивирусные программные комплексы:

- антивирус Касперского (AVP) Personal;
- антивирус Dr. Web;
- антивирус Symantec Antivirus;
- антивирус McAfee;
- антивирусAntiVir Personal Edition.

Наиболее мощными антивирусными комплексами из линеек производителей антивирусов, входящими в класс InternetSecurity, на сегодняшний день являются:

- Panda Internet Security;
- Dr.Web 7.0 SecuritySpace;
- Comodo Internet Security Pro;
- Kaspersky Internet Security;
- Emsisoft Internet Security Pack;
- Eset NOD32;
- Avast 7 Internet Security;
- Avast 7 Free Antivirus;
- Avira Internet Security;
- Avira Free Antivirus.

Программные закладки и методы защиты от них

Угроза внедрения программных закладок актуальна практически для любых многопользовательских КС.

Программные закладки классифицируются:

- по методу внедрения;
- по назначению.

1. По методу внедрения в компьютерную систему программные закладки делятся на:

– программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера (их средой обитания, как правило,

является BIOS – набор программ, записанных в виде машинного кода в постоянном запоминающем устройстве – ПЗУ);

– загрузочные закладки, ассоциированные с программами начальной загрузки, которые располагаются в загрузочных секторах (из этих секторов в процессе выполнения начальной загрузки компьютер считывает программу, берущую на себя управление для последующей загрузки самой операционной системы);

– драйверные закладки, ассоциированные с драйверами (то есть файлами, в которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);

– прикладные закладки, ассоциированные с прикладным программным обеспечением общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);

– исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаще всего эти модули представляют собой пакетные файлы, то есть файлы, которые состоят из команд операционной системы, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера);

– закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек);

– замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового и развлекательного назначения.

2. По основным действиям деструктивного характера, осуществляемым в компьютерной системе, программные закладки делятся на:

– закладки, осуществляющие копирование пользовательской конфиденциальной информации, которая находится в оперативной памяти, внешней памяти системы, либо в памяти другой системы, подключенной по локальной или глобальной сети;

– закладки, осуществляющие изменение алгоритмов функционирования системных, прикладных и служебных программ;

– закладки, осуществляющие изменение режимов работы программного обеспечения.

Защита от программных закладок осуществляется в следующих вариантах:

1. Защита от внедрения закладок в большинстве случаев осуществляется путем создания изолированного персонального компьютера, защищенного от проникновения программных закладок извне. Для того чтобы считаться изолированным, компьютер должен удовлетворять следующим условиям:

– BIOS не должен содержать программных закладок;

– установленная операционная система должна быть проверена на наличие программных закладок;

– должна быть установлена неизменность BIOS и операционной системы;

– на ПК не должны были запускаться и не запускаются программы, которые не прошли проверку на наличие в них программных закладок;

– должен быть исключен запуск проверенных программ вне ПК.

2. Выявление внедренных программных закладок осуществляется путем обнаружения признаков их присутствия в системе. Эти признаки делятся на:

– качественные и визуальные – это признаки, которые могут быть идентифицированы пользователем во время работы с системой. Это могут быть как отклонения от привычной работы системы, так и изменения в пользовательских и системных файлах. Наличие данных признаков свидетельствует о необходимости проведения проверки на наличие программных закладок в системе;

– обнаруживаемые средствами диагностики, которые идентифицируются специальным тестовым программным обеспечением, сигнализирующим о наличии вредоносного программного кода в системе.

3. Удаление внедренных закладок. Данный метод зависит от метода их внедрения в систему. При обнаружении программно-аппаратной закладки необходимо перепрограммировать ПЗУ компьютера. При обнаружении загрузочной, драйверной, прикладной, замаскированной закладки или закладки-имитатора необходимо произвести их замену на соответствующее программное обеспечение от доверенных источников. При обнаружении исполняемой закладки следует убрать текст закладки из исходного текста программного модуля и откомпилировать модуль заново.

Вопросы для самоконтроля

1. Что такое вредоносная программа и какие виды вредоносных программ существуют?
2. По каким признакам классифицируются компьютерные вирусы?
3. Перечислите основные каналы распространения компьютерных вирусов и других вредоносных программ.
4. Перечислите основные методы обнаружения компьютерных вирусов и дайте краткую характеристику каждого из них.
5. Что такое антивирусная программа и на какие виды антивирусные программы подразделяются?
6. Перечислите наиболее известные антивирусные программы и комплексы.
7. Что собой представляют программные закладки и как они классифицируются?
8. Какие существуют способы защиты от программных закладок?

8. БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ-РЕСУРСОВ

Анонимное использование интернет-ресурсов

Анонимность в Интернете – это достаточно актуальная тема для каждого пользователя Интернета, так как существует очень много способов узнать личную информацию о пользователе по его IP-адресу или другим характеристикам интернет-соединения.

Зная IP-адрес пользователя, можно узнать его реальное место нахождения и проследить все его действия, совершенные, например, с домашнего компьютера. Владелец любого удаленного сервера или сайта в Интернете может точно определить, что пользователь делал на его сайте. Например, какие товары просматривал, но не купил, какие смотрел или скачал картинки, фотографии, фильмы и музыку, а также какой объем занял его трафик. И многое другое.

Так же в последнее время все больше и больше ресурсов предоставляют человеку различную информацию в зависимости от места проживания. Так, например, многие информационные деловые проекты США не показывают самые важные данные выходцам из других стран. Также наблюдается тенденция усиления слежки в Сети.

Выбор провайдера. Маскировка IP-адреса

Принцип адресации пересылаемых пакетов информации следующий. Когда пользователь набирает в строке браузера какой-нибудь адрес, то сначала запрос отправляется на сервер DNS, который преобразует строку символов в набор из 32 нулей и единиц, то есть **IP-адрес**, использующийся для маршрутизации. Зная этот адрес, злоумышленник может выведать о пользователе очень многое. Например, его реальное местонахождение. Делается это с помощью сервиса **whois**, который по IP-адресу легко определяет провайдера пользователя.

Существуют следующие способы маскировки (скрытия) IP-адреса:

1. Использование **анонимного прокси-сервера** (**anonymous http proxy server**), который исполняет роль посредника между пользователем и конечной целью его запроса. Пользователь отправляет запрос, прокси-сервер его обрабатывает и выдает за свой, после получения ответа прокси-сервер этот ответ также обрабатывает и передает на компьютер пользователя.

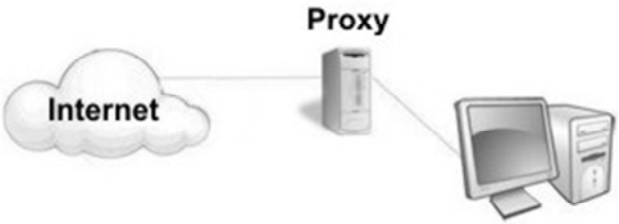

Рис. 4

Прокси-сервера применяются в основном для анонимного серфинга в Интернете, а сами прокси получили название **HTTP (HTTPS) proxy** серверов. Чтобы анонимно перемещаться по страницам web-сайтов, в популярных браузерах имеется специальный инструментарий, через который их можно настроить на использование прокси-серверов. Для этого в параметрах подключения пользовательского web-браузера указываются настройки прокси-сервера: имя и порт.

Недостатки прокси серверов: многие прокси-серверы в заголовки своих запросов могут вставлять IP-адрес пользователя, то есть быть не анонимными; значительно уменьшают скорость загрузки web-страниц; прокси серверы очень нестабильны, а время жизни прокси-сервера может составить от 1-го до 24-х часов. Поэтому прокси-сервера перед использованием обязательно нужно проверять на работоспособность и анонимность. Для этого существуют специальные программы или сервисы в Интернете на специализированных сайтах. Например, программа **Proxy Checker** (сайт **http://www.freeproxy.ru/**) позволяет брать списки proxy из файлов разных форматов (HTML и TXT), проверять proxy на анонимность, проверять HTTP proxy на поддержку FTP, HTTPS и proxy chain (proxy chain – поддержка работы в цепочке из нескольких прокси).

Чтобы узнать IP-адрес, который присвоил вам ваш провайдер, перейдите, например, по ссылке: http://checkip.dyndns.org/. Затем установите в интернет-браузере настройки прокси и зайдите еще раз. Если IP-адрес будет другим, значит прокси действительно анонимный.

2. Использование **программ-анонимайзеров** (**anonymizer**), которые выглядят как обычный поисковик, только вместо слов/фраз в них нужно вводить URL того сайта, который необходимо посмот-

реть. Программы-анонимайзеры также используют анонимные прокси-серверы, но поиск, проверку, подключение к анонимным прокси-серверам выполняют самостоятельно и снабжены собственным web-интерфейсом.

Недостатки использования анонимайзеров: может существенно уменьшиться скорость загрузки web-страниц; на некоторых анонимайзерах не исключены проблемы с отображением русскоязычного текста; сейчас практически невозможно отыскать бесплатный прокси-сервер.

3. Использование **socks-протоколов** (**socks proxy server**) является самым надежным на данный момент способом сокрытия IP-адреса. Принцип действия напоминает принцип действия прокси-серверов и выглядит так: socks-сервер принимает данные от компьютера пользователя, отправляет их на web-сервера, потом перенаправляет ответную информацию обратно к пользователю. Но есть и следующие принципиальные отличия технологии socks-серверов и прокси-серверов: «общение» клиентского компьютера и socks-сервера происходит не по общепринятым, а по специальным протоколам (**socks4**, **socks5** и т. д.). В результате передача IP-адреса пользователя невозможна в принципе. Кроме того, socks-сервер сам преобразовывает информацию от пользователя в запросы для общепринятых протоколов. Таким образом, ни один сервер никогда «не догадается», что отправляет данные не конечному пользователю, а только посреднику в лице socks-сервера. К тому же работать с технологией socks очень удобно. Например, установив и запустив программу **Socks-Cap** (русский аналог – программа **FreeCap**), пользователю останется лишь выбрать софт, для которого он хотел бы использовать анонимное соединение (например, **The Bat** или **Internet Explorer**) и ввести адрес и порт socks-сервера. Можно даже создавать цепочки SOCKS-серверов (SOCKS Chain), что еще больше повышает степень анонимности.

4. Использование **VPN-технологии** (**Virtual Private Network**) – технологии, позволяющей подменить IP-адрес без использования прокси-сервера. С помощью VPN-подключения устанавливается своеобразный интернет-тоннель между компьютером пользователя и удаленным VPN-сервером. Все действия в сети Интернет будут выполняться через этот тоннель и все данные (как входящие, так и исходящие) будут также направляться через тоннель VPN-

подключения. Образуемое тоннелем SSL-соединение шифрует все данные и информацию и надежно защищает их от несанкционированного доступа и кражи. Даже провайдер, через которого компьютер пользователя подключен к интернету, ничего не сможет узнать о действиях пользователя в сети. Соединившись с удаленным VPN-сервером, все обращения пользователя к посещаемым серверам и страницам в сети будут происходить от имени этого сервера. Сервера и web-страницы, посещаемые пользователем, будут видеть чужой IP-адрес удаленного VPN-сервера, а не реальный IP-адрес самого пользователя.

Достоинства: VPN-подключение лишено недостатков, присущих анонимным прокси и socks-прокси серверам. Анонимное интернет-соединение стабильно, качественно, обладает высокой скоростью, канал передачи данных надежно защищен и зашифрован, а, кроме того, анонимная работа обеспечивается практически на всех протоколах: http, https, ftp, smtp, pop, imap, upload и download файлов и др.

Недостатки: услуги анонимных VPN-сервисов платные.

Использование специализированных программ и сервисов

Чтобы обеспечить анонимность своего пребывания в сети Интернет можно использовать следующие специальные программы (бесплатные):

1) сервис **HideMyAss** обеспечивает анонимность в Сети, скрывая пользовательский IP-адрес;

2) популярное приложение **Tor Project** (бесплатное), представляющее программный комплекс для обеспечения анонимного статуса при серфинге сайтов;

3) **Surf Anonymous Free** – программа, которая защищает пользователя от небезопасных сайтов, предотвращает отслеживание и мониторинг сетевого трафика;

4) программа **Steganos Internet Anonym**, которая строит длинные цепочки прокси, надежно скрывая пользовательский IP-адрес, а также блокирует все скрипты (cookies, Active-X и Java-скрипты), способные раскрыть информацию о пользователе и его местоположении владельцам посещенных сайтов;

5) программа **Complete Anonymous Web Surfing** позволяет скрыть IP-адрес пользователя при просмотре web-страниц, устанав-

ливая подключение через один из имеющихся в наличии прокси-серверов;

6) сервис **TryCatchMe** («Попробуй поймать меня») поможет зайти на заблокированный администратором сайт и сохранить практически все конфиденциальные данные при себе.

Безопасное использование электронной почты (E-mail). Выбор почтового клиента

Основными угрозами информационной безопасности при использовании электронной почты являются:

1) блокирование электронного почтового ящика;

2) потеря почтового сообщения, когда сообщение не доходит до адресата;

3) перехват электронной почтовой корреспонденции, приводящий к нарушению конфиденциальности информации, передаваемой по электронной почте;

4) несанкционированный доступ к электронному почтовому ящику (взлом электронного почтового ящика), следствием которого может быть нарушение целостности, доступности и конфиденциальности находящихся в нем почтовых сообщений;

5) несанкционированный доступ к компьютеру пользователя электронной почты, следствием которого может быть нарушение целостности, доступности и конфиденциальности хранящихся в компьютере почтовых сообщений либо утечка информации, которая может быть использована для несанкционированного доступа к электронному почтовому ящику;

6) подмена имени, электронного и/или IP-адреса отправителя в электронном почтовом сообщении или удаление имени и адреса отправителя;

7) формирование подложного сообщения от имени адресата, известного получателю сообщения;

8) несанкционированная рассылка сообщений – спам;

9) внедрение в компьютер вредоносных программ, полученных с электронным почтовым сообщением;

10) анализ почтового трафика, позволяющий определить наличие связи между отправителем и получателем электронной корреспонденции;

11) атаки на почтовые серверы, способные приводить к потере целостности, конфиденциальности и доступности почтовых сообщений.

Компьютерные вирусы распространяются по электронной почте под видом вложений, прикрепленных к письмам. Вирус активизируется, если пользователь открывает это вложение.

В первую очередь, следите, чтобы у вас были установлены самые последние обновления программ.

Нелишним будет установить персональный межсетевой экран (firewall). В нем следует указать исчерпывающий список программ и доступных им портов и сервисов. Как только какая-либо незнакомая программа попытается отправить почту, она тут же будет обнаружена, и зараза не распространится с Вашего компьютера дальше.

Кроме того, отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы (обращение к файлам, загрузочной области диска, системному реестру и т. п.), способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.

Почтовый клиент – это программное обеспечение, позволяющее подключиться к учетной записи электронной почты и загружать электронные письма на свой компьютер, создавать письма, которые можно отправить либо сразу, либо позже. Почтовый клиент хранит все сообщения на компьютере пользователя, что дает возможность сортировать и управлять сообщениями.

Электронная почта одна из самых доступных по отношению к спаму и многие компании пользуются этим. Они собирают адреса и отправляют нежелательную почту каждому из списка. Такие сообщения могут быть заражены вирусами или содержать программы-шпионы.

Некоторые почтовые клиенты специализированы для проверки писем на присутствие вредоносных программ. Очень часто клиенты электронной почты имеют папку «Спам», в которой хранятся письма, которые возможно были разосланы программами-роботами, и не имеют полезной информации.

Защита от спама

Спам – это массовые неадресные рекламные рассылки по электронной почте.

Способы распространения спама:

1) **электронная почта**. Самый большой поток спама распространяется через электронную почту (e-mail). Спамеры собирают e-mail-адреса с помощью специального робота или вручную (редко), используя веб-страницы, конференции Usenet, списки рассылок, электронные доски объявлений, гостевые книги и чаты. Программа-робот способна собрать за час тысячи адресов и создать из них базу данных для дальнейшей рассылки по ним спама. Некоторые компании занимаются только сбором адресов, а базы потом продают или продают спамерам e-mail-адреса своих клиентов, заказавших у них товары или услуги по электронной почте. Другой способ получения работающих e-mail-адресов – это генерация адресов случайным образом по заданным шаблонам (от тысячи до миллиона), а потом их проверка специальной программой-валидатором на их валидность (существование);

2) **мгновенные сообщения**. С развитием служб доставки мгновенных сообщений, спамеры стали их использовать для своих целей. Многие из этих служб предоставляют список пользователей, которым можно воспользоваться для рассылки спама;

3) **социальные сети и сайты знакомств**. Значительная часть приходящих пользователям популярных социальных сетей и сайтов знакомств личных сообщений является спамом, который часто рассылается от имени пользователей, логины и пароли которых попали в руки спамеров. Кроме личных сообщений также могут использоваться приглашения в группы или сообщества, заявки на «дружбу», «стены»/«гостевые книги» и т. д.;

4) **блоги, вики, форумы, доски объявлений**. Спам, размещенный на веб-сайтах, на которых можно оставлять комментарии (форумы и блоги) или которые можно свободно редактировать (вики), труднее удалить, так как сообщения в форумах и блогах могут редактировать только привилегированные пользователи – соответственно, рядовой участник должен связаться с кем-нибудь из них). Другая разновидность спама в блогах – автоматическое внесение пользователей в список «друзей» без знакомства с их персональными страницами, с целью искусственного повышения собственного рей-

тинга путем получения «взаимной» дружбы, либо привлечения внимания к сетевой рекламе. Спам на досках объявлений – это размещение информации коммерческого и полукоммерческого содержания в виде объявлений, где каждое слово выглядит как гиперссылка. Иногда в одном объявлении можно увидеть более десятка ссылок, ведущих на разные страницы;

5) **поисковый спам** – страницы и web-сайты, созданные с целью манипулирования результатами, выданными поисковыми системами, например *дорвеи* – страницы с ключевыми словами и автоматическим перенаправлением на «нужный» сайт;

6) **сетевые сообщения**. Иногда спам рассылают по локальной сети через встроенную в Microsoft Windows службу Messenger. Такие сообщения появляются в виде всплывающих окон.

Методы защиты от спама:

1) ручная или автоматическая фильтрация почты по заголовкам. В принципе, любой пользователь может перейти с протокола POP3 на IMAP4 или на Web-интерфейс и оценивать письма только по их заголовкам, не получая текста. Во многих почтовых программах можно настроить автоматическую фильтрацию по заголовкам писем. Однако в последнем случае требуется очень тонкая и вдумчивая подгонка условий оценки и можно получить много нареканий от своих нерадивых корреспондентов по сбоям в работе такого фильтра;

2) самыми надежными являются специальные службы фильтрации, которые могут находиться у почтового провайдера или на отдельном сервере (последние, как правило, платные). В некоторых случаях вся почта отправляется на определенный адрес, где фильтруется, и к пользователю приходит уже чистой. Этот метод – самый простой для пользователя, но, как правило, и наименее контролируемый (то есть велика вероятность, что может потеряться часть полезной корреспонденции, о чем никто никогда не узнает);

3) можно применять входные фильтры, основанные на анализе IP-адреса хоста, передающего спам (который можно узнать, например, по отзывам пострадавших), и использовать общие базы данных с адресами таких спамеров (DNSBL – DNS Black Lists). Однако сегодня это уже малоэффективный способ борьбы с современными методами спама;

4) существует фильтрация на основе автоматического пополнения access-листа адресами спамеров. Например, при такой фильтра-

ции может использоваться встречный анализ подозрительности отправляющего хоста, однако данный фильтр плох тем, что требует постоянного контроля и тонкой настройки. Причем первое письмо от потенциального спамера он в любом случае пропустит, что делает его работу малоэффективной в современных условиях;

5) существуют программы или встраиваемые модули для анализа содержимого письма. Программы для такой проверки (их может быть несколько) принимают информацию от почтовой программы, а возвращают, как правило, свою оценку и рекомендацию к дальнейшему действию.

Вопросы для самоконтроля

1. Что такое IP-адрес пользователя и каков принцип адресации пересылаемых пакетов информации в сети?
2. Перечислите способы маскировки (сокрытия) IP-адреса в сети.
3. Какие существуют основные угрозы информационной безопасности при использовании электронной почты?
4. Что такое спам и какие существуют способы распространения спама?
5. Какие методы защиты от спама существуют в настоящее время?

9. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Криптография как наука. Основные понятия

Криптография – это фундаментальная наука, изучающая методы преобразования информации, направленные на сокрытие ее содержания.

Слово «криптография» (cryptography) происходит от греческих слов «kryptus» – тайный, «graphein» – писать, то есть дословно «тайнопись».

Криптоанализ – это наука, изучающая методы взлома шифров.

Криптология – наука, которая занимается изучением шифров и их стойкости.

Криптология = Криптография + Криптоанализ

История криптографии насчитывает несколько тысячелетий. Первые системы шифрования появились одновременно с письменностью в четвертом тысячелетии до н. э.

Краеугольный камень криптографии – **шифрование** (то есть криптографическая обработка информации с помощью одного из алгоритмов).

Исходное сообщение называется *открытым текстом*. Зашифрованное сообщение называется *шифротекстом*.

Любой алгоритм шифрования должен быть дополнен алгоритмом расшифрования, чтобы привести зашифрованный текст в исходный вид.

Дешифрование – восстановление исходного текста без знания ключа.

Пара процедур – шифрование и расшифрование – называется **криптосистемой**.

Сегодня широко распространено два типа шифрования:

1. Традиционное, или симметричное (с секретным ключом).
2. Асимметричное (с открытым ключом).

В симметричных криптосистемах для шифрования и для дешифрования используется один и тот же ключ (или же ключ для дешифровки просто вычисляется по ключу шифровки).

В системах с открытым ключом используются два ключа – открытый и закрытый, – которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Процесс традиционного шифрования включает две составляющие:

1. Алгоритм шифрования.
2. Ключ – значение, не зависящее от открытого текста.

Результат, достигаемый при выполнении алгоритма, зависит от применяемого ключа. Изменение ключа приводит к изменению шифрованного текста.

Надежность традиционного шифрования определяется с помощью нескольких факторов:

1. Сложность алгоритма шифрования (алгоритм должен быть достаточно сложным, чтобы невозможно было расшифровать сообщение при наличии только шифрованного текста).

2. Секретность ключа – основной фактор надежности традиционного шифрования. Сам алгоритм может быть несекретным.

В традиционной (классической) криптографии принято фундаментальное правило, сформулированное в 19 веке, – правило Керкхоффа: «Стойкость шифра должна определяться только секретностью ключа».

Эта особенность традиционного шифрования обуславливает его широкую популярность и признание. Так как нет необходимости хранить в секрете алгоритм, то производители могут реализовать алгоритмы шифрования в виде дешевых общедоступных микросхем, которыми оснащены многие современные системы.

Модель традиционной криптосистемы

Теоретические основы традиционной модели симметричной криптосистемы впервые были изложены в 1949 году в работе Клода Шеннона.

Источник создает сообщение в форме открытого текста:

$$X = [x_1, x_2, \ldots, x_m].$$

Элементами x_i открытого текста X являются символы некоторого конечного алфавита A, состоящего из n символов:

$$x_i \cdot A.$$

Традиционно использовался алфавит из 26 букв английского языка, но сегодня чаще применяется двоичный алфавит {0,1}.

Для шифрования генерируется ключ в форме:

$$K = [\kappa_1, \kappa_2, \ldots, \kappa_j].$$

Если ключ генерируется там же, где и само сообщение, то его необходимо переправлять получателю по секретным каналам. Либо ключ создается третьей стороной, которая должна защищенным способом обеспечить доставку ключа отправителю и получателю сообщения.

Если есть X и K, с помощью алгоритма шифрования формируется шифрованный текст

$$Y = [y_1, y_2, \ldots, y_n].$$

Это можно записать в виде формулы:

$$Y = E_k(X).$$

Y получается путем применения алгоритма шифрования E к открытому тексту X при использовании ключа K.

Обратное преобразование:

$$X = D_k\,(Y),$$

где D – алгоритм (или функция) расшифрования;

k – ключ расшифрования (дополнительный параметр функции расшифрования).

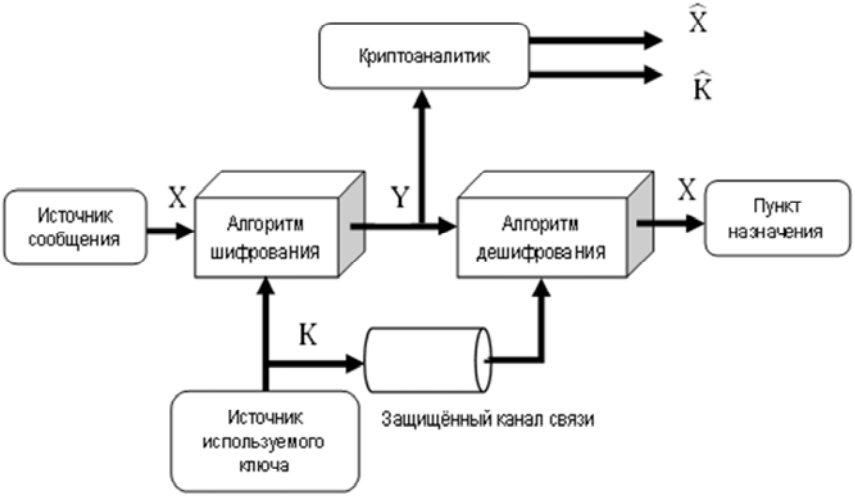

Рис. 5

Типы криптосистем

Классификация криптографических систем строится на основе следующих трех характеристик:

1) число применяемых ключей;

2) тип операций по преобразованию открытого текста в шифрованный;

3) метод обработки открытого текста.

1. По числу применяемых ключей различают:

- *симметричные* криптосистемы;
- *асимметричные* криптосистемы.

Если отправитель и получатель используют один и тот же ключ, система шифрования называется *симметричной* (системой с одним ключом, системой с секретным ключом, схемой традиционного шифрования. Например, DES, CAST, RC5, IDEA, Blowfish, классические шифры.

Если отправитель и получатель используют разные ключи, система называется *асимметричной* (системой с двумя ключами, схемой шифрования с открытым ключом). Например, RSA, Эль-Гамаля.

2. По типу операций по преобразованию открытого текста в шифрованный различают:

– *подстановочные шифры* – шифрование основано на замещении каждого элемента открытого текста (бита, буквы, группы битов или букв) другим элементом (Цезаря, Плейфейера, Хилла);

– *перестановочные шифры* – шифрование основано на изменении порядка следования элементов открытого текста (лесенка, перестановка столбцов);

– *продукционные шифры* – шифрование основано на комбинации нескольких операций замены и перестановки. Продукционные шифры применяются в большинстве реальных современных систем шифрования (DES).

3. По методу обработки открытого текста различают:

– *блочные шифры* – это шифры, в которых логической единицей шифрования является некоторый блок открытого текста, после преобразования которого получается блок шифрованного текста такой же длины. Например, DES, шифр Файстеля.

– *поточные шифры* – подразумевают шифрование всех элементов открытого текста последовательно, одного за другим (бит за битом, байт за байтом). Примерами классических поточных шифров являются шифры Виженера (с автоматическим выбором ключа) и Вернама.

Блочные шифры изучены гораздо лучше. Считается, что они обладают более широкой областью применения, чем поточные. Большинство сетевых приложений, в которых применяется схема традиционного шифрования, используют блочные шифры.

Электронная цифровая подпись и ее применение

Электронная цифровая подпись (**ЭЦП**) – это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося.

ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам.

ЭЦП обеспечивает следующие функции:

1) удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

2) не дает этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

3) гарантирует целостность подписанного текста.

ЭЦП представляет собой небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже – отдельно) с подписываемым с ее помощью документом.

Механизм ЭЦП состоит из двух процедур:

– получение (простановка) подписи с помощью секретного ключа автора документа;

– проверка ЭЦП при помощи открытого ключа автора документа.

Алгоритм получения ЭЦП под документом следующий:

1. Вычисление хеш-значения (хеш-функции) для документа.

2. Шифрование хеш-значения с помощью секретного ключа автора документа (полученный шифротекст и будет являться ЭЦП).

Алгоритм проверки ЭЦП под документом следующий:

1. Вычисление хеш-значения для документа.

2. Расшифрование ЭЦП с помощью открытого ключа автора документа.

3.Сравнение вычисленного и расшифрованного хеш-значений для документа.

Хеш-значения (хеш-функции) являются одним из важных элементов криптосистем на основе ключей. Их относительно легко вычислить, но почти невозможно расшифровать. Хеш-функция имеет исходные данные переменной длины и возвращает строку фиксированного размера (иногда называемую дайджестом сообщения – MD), обычно 128 бит. Хеш-функции используются для обнаружения модификации сообщения (то есть для электронной подписи).

Перед получением ЭЦП в подписываемый документ должны быть включены дополнительные сведения:

– дата и время простановки подписи;

– срок окончания действия секретного ключа данной подписи;

– реквизиты (фамилия, имя, отчество подписывающего лица, его должность и название представляемой организации);

– идентификатор секретного ключа (для возможности выбора лицом, проверяющим ЭЦП, нужного открытого ключа).

Известны следующие системы ЭЦП:

– на основе алгоритмов симметричного шифрования (шифрование и расшифровывание производится закрытым ключом);

– на основе алгоритмов асимметричного шифрования (зашифровывается закрытым ключом, а расшифровывается открытым ключом).

В таможенных органах Республики Беларусь используется асимметричный алгоритм шифрования, но при этом проблемой является защита открытых ключей от подмены злоумышленником и организация отзыва ключа в случае его компрометации. Защита ключей от подмены осуществляется с помощью сертификатов, которые позволяют удостоверить заключенные в нем данные о владельце и его открытый ключ подписью какого-либо доверенного лица.

В Республике Беларусь получить сертификат открытого ключа можно в подразделении Национального центра электронных услуг – Республиканском удостоверяющем центре государственной системы управления открытыми ключами, который начал работать с 2014 года и имеет региональные представительства в крупных городах Беларуси.

Благодаря высокой степени надежности и легкости использования, ЭЦП нашла свое применение для защиты сведений, передаваемых по открытым каналам передачи данных, при использовании системы электронного декларирования в таможенных органах Республики Беларусь.

Компьютерная стенография и ее применение

Применение методов криптографии позволяет скрыть от непосвященных содержание конфиденциальной информации, но не способно скрыть самого факта ее наличия или передачи. Методы стенографии направлены на скрытие самого присутствия конфиденциальной информации.

Применительно к стенографии различают сообщение (объект, существование и содержание которого должно быть скрыто) и контейнер (объект, в котором скрывается сообщение). При помещении сообщения в контейнер может использоваться секретный ключ, определяющий порядок помещения сообщения в контейнер. Этот же ключ должен быть задан при извлечении сообщения из контейнера.

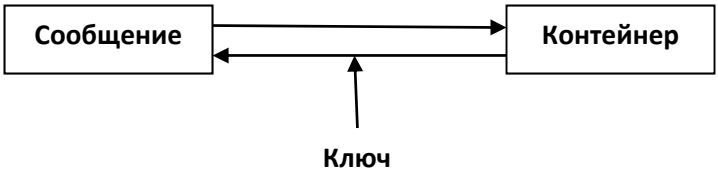

Рис. 6

Большое развитие получили методы стеганографии в последние годы в связи с бурным развитием компьютерных технологий.

Принципы компьютерной стеганографии:

– обеспечение аутентичности и целостности файла-сообщения;

– открытость методов компьютерной стеганографии;

– сохранение основных свойств файла-контейнера после помещения в него сообщения (после этого файл-контейнер можно открывать, сжимать, восстанавливать без потери качества и изменения содержания информации в контейнере);

– сложность извлечения сообщения из файла контейнера при известности факта скрытия сообщения, но без знания ключа.

Методы компьютерной стеганографии делятся на две основные группы:

1. Методы, использующие специальные свойства форматов электронных документов: зарезервированные для дальнейшего применения поля; специальное форматирование текстовых документов; неиспользуемые места дисковой памяти; имитирующие функции для генерации осмысленного текста файла-контейнера для скрываемого сообщения и др.

2. Методы, использующие естественную избыточность оцифрованных графических изображений, звука и видеоинформации. Например, полноцветные графические файлы в формате RGB кодируют каждую точку (пиксель) изображения тремя байтами для представления соответственно красной, зеленой и синей составляющих. Изменение каждого из трех младших битов приведет к изменению цветовых характеристик данной точки изображения менее чем на 1 %, что абсолютно незаметно для человеческого глаза. Этот метод позволяет скрыть в графическом файле размером 800 Кб сообщение размером до 100 Кб.

Основные задачи, которые могут решаться с помощью методов компьютерной стеганографии:

– защита от несанкционированного доступа к конфиденциальной информации;

– преодоление систем сетевого мониторинга и управления сетевыми ресурсами (например, систем промышленного шпионажа, регистрирующих частоту обмена конфиденциальными сообщениями даже при отсутствии возможности их расшифрования);

– камуфлирование конфиденциального программного обеспечения (защита его от использования незарегистрированными пользователями путем скрытия в мультимедийных файлах);

– защита авторских прав создателей электронных документов путем нанесения на файлы с этими документами (фото, аудио и видеоматериалами) специальной метки (водяного знака), распознаваемого только специальным обеспечением.

Типы криптоатак и стойкость алгоритмов

Процесс воссоздания открытого текста (X) и/или ключа (K) называется **криптоанализом**.

Алгоритм шифрования считается раскрытым, если найдена процедура, позволяющая подобрать ключ за реальное время.

Сложность алгоритма раскрытия является одной из важных характеристик криптосистемы и называется криптостойкостью.

Схема шифрования называется абсолютно стойкой (или безусловно защищенной), если шифрованный текст не содержит информации, достаточной для однозначного восстановления открытого текста.

Это означает, что, независимо от того, сколько времени потратит противник на расшифровку текста, ему не удастся расшифровать его просто потому, что в шифрованном тексте нет информации, требуемой для восстановления открытого текста.

Максимум, что может дать алгоритм шифрования, это выполнение хотя бы одного из следующих условий:

1) стоимость взлома шифра превышает стоимость расшифрованной информации;

2) время, которое требуется для взлома шифра, превышает время, в течение которого информация актуальна.

Если схема шифрования соответствует обоим указанным критериям, она называется защищенной по вычислениям.

Все формы криптоанализа для схем традиционного шифрования разрабатываются на основе того, что некоторые характерные особенности структуры открытого текста могут сохраняться при шифровании, проявляясь в шифрованном тексте.

Криптоанализ для схем с открытым ключом базируется на совершенно другом – на том, что математические зависимости, связывающие пары ключей, дают возможность с помощью логических рассуждений, зная один из ключей, найти второй.

Основные типы криптоатак:

1. *Атака на основе шифротекста*. Криптоаналитик располагает шифротекстами нескольких сообщений, зашифрованных одним и тем же алгоритмом шифрования и, возможно, ключом.

2. *Атака на основе открытого текста*. Криптоаналитик располагает доступом не только к шифротекстам нескольких сообщений, но и открытому тексту этих сообщений. Его задача состоит в определении ключа или ключей, чтобы он мог расшифровать другие сообщения.

3. *Атака на основе подобранного открытого текста* (криптоаналитик может выбирать открытый текст для шифрования). Во многих сообщениях используются стандартные начала и окончания, которые могут быть известны криптоаналитику (атаки 2, 3).

В этом отношении особенно уязвимы шифрованные исходные коды программ из-за частого использования ключевых слов (define, struct, else, return и т. д.). Те же проблемы и у шифрованного исполняемого кода: функции, циклические структуры и т. д.

4. *Лобовое вскрытие* (лобовая атака, метод «грубой силы» – путем перебора всех возможных ключей).

5. *Бандитский криптоанализ*. Для получения ключа «криптоаналитик» прибегает к угрозам, шантажу или пыткам. Возможно также взяточничество, которое называется вскрытием с покупкой ключа. Это очень мощные и, зачастую, самые эффективные методы взлома алгоритма.

Вопросы для самоконтроля

1. Дайте определение таких понятий, как криптография, криптоанализ и криптология?
2. Что такое шифрование и дешифрование, какие способы шифрования распространены в настоящее время?
3. В чем заключается суть модели традиционной криптосистемы?
4. Как классифицируются криптосистемы?
5. Что такое электронная цифровая подпись (ЭЦП) и какие функции она обеспечивает?
6. Каковы алгоритмы получения электронной цифровой подписи и ее проверки под документом?
7. Какие системы ЭЦП существуют в настоящее время и какие из них используются в таможенных органах Республики Беларусь?
8. Что такое компьютерная стенография и где она используется?
9. Какая схема шифрования называется абсолютно стойкой и каким условия она должна удовлетворять?
10. Что такое криптоатака и какие типы криптоатак существуют?

10. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТАМОЖЕННЫХ ОРГАНАХ РЕСПУБЛИКИ БЕЛАРУСЬ

Применяемые в таможенных органах информационные технологии обеспечивают реализацию информационных процессов – процессов сбора, обработки, накопления, хранения, поиска и распространения информации. Информационные системы таможенных органов представляют собой организационно упорядоченные совокупности информационных ресурсов и информационных технологий, в основном с использованием средств вычислительной техники и связи, обеспечивающие эффективную реализацию процедур таможенного оформления и таможенного контроля. Они интегрируются и взаимодействуют с информационными системами участников внешнеэкономической деятельности (далее – ВЭД), других организаций и государственных органов, предназначенными для представления сведений в электронной форме, с сетями общего пользования.

От эффективности деятельности таможенных органов в информационной сфере существенно зависит эффективность обеспечения экономической безопасности Республики Беларусь.

Таможенные органы, контролирующие международные грузопотоки и управляющие ими, способствуют социально-экономическому развитию государства путем защиты внешней торговли от факторов, способных нанести ущерб экономике.

В целях обеспечения современного уровня таможенной службы Республики Беларусь, соответствующего лучшим международным стандартам, необходимо постоянно модернизировать единую автоматизированную информационную систему таможенных органов. В настоящее время создана и функционирует Национальная автоматизированная система таможенного декларирования (далее – НАСТД).

Услуги по электронному декларированию предоставляются участникам ВЭД по всей территории страны. Более 80 процентов поставок экспортных товаров и более 7 процентов импортных поставок оформляется в виде электронных документов, временно вывозимых товаров – 90 процентов.

В рамках Таможенного союза создается единая система и единая база данных выданных лицензий. В систему включены Минторг, Минздрав, МВД, республиканское унитарное предприятие по надзору за электросвязью «БелГИЭ» Минсвязи, Минприроды.

Создана основа для расширения информационного взаимодействия, в том числе между министерствами и организациями, выдающими разрешения на перемещение товаров через таможенную границу, ограниченных к такому перемещению. Реализуется Рекомендация Европейской экономической комиссии ООН № 33 по повышению эффективности обмена информацией между участниками международной торговли и правительственными учреждениями (реализация принципа «одно окно» при таможенном декларировании).

В перспективе предусматривается реализация в пунктах пропуска через Государственную границу Республики Беларусь принципа «одна остановка», также основанного на организации информационного взаимодействия контрольных служб пункта пропуска между собой и участниками внешней торговли, в настоящее время трансформировавшегося в принцип «интегрированное управление границей». Государственный таможенный комитет приступил к реализации этого принципа через разработку и внедрение Автоматизированной системы управления процессами контроля в автодорожном пункте пропуска. Внедрение этой системы показало, что необходимо организовывать информационный обмен между контрольными службами не только на локальном уровне, но и на уровне центральных аппаратов контрольных служб, а также обмен информацией между таможенной службой и грузоперевозчиками, импортерами и экспортерами.

Создана информационная система учета движения таможенных платежей, предназначенная для автоматизированного формирования и ведения лицевых счетов субъектов ВЭД, расчета и анализа таможенной задолженности, контроля своевременности и полноты зачисления в бюджет государства сумм платежей, взимаемых таможенными органами.

Также были построены линейные и станционные сооружения от пунктов пропуска через Государственную границу Республики Беларусь до районных узлов электросвязи РУП «Белтелеком», модернизированы узлы связи и телекоммуникаций таможен, Минской центральной таможни. Это позволило организовать выделенные цифровые каналы передачи данных от пунктов пропуска до таможен и от таможен до Минской центральной таможни – Центра обработки данных таможенных органов.

Развитие информационного общества предполагает предоставление государственных услуг и исполнение государственных функ-

ций в электронном формате, что является одним из признаков электронного правительства.

Таможенные органы также стремятся к переходу на электронный документооборот. Среди приоритетных задач таможенных органов большинства стран мира указано внедрение интернет-технологии при электронном представлении сведений, а так же полный переход на безбумажный оборот и технологию представления в электронном виде таможенной декларации и документов, на основе которых она заполнена.

При рассмотрении вопросов электронного декларирования, передачи информации от участника ВЭД в таможенный орган в электронном виде, а также деятельности различных онлайн-сервисов таможенной службы, следует учитывать, что это имеет как положительные, так и отрицательные аспекты. Безусловно, переход к электронному документообороту способствует ускорению проведения таможенных операций, снижению коррупции и упрощению взаимодействия с таможенными органами. Однако, в век «высоких технологий» велик риск незаконного проникновения в информационную среду таможенных органов. В связи с этим возрастает значение информационной безопасности таможенных органов.

Образование Таможенного союза, вступление в силу Таможенного кодекса ЕАЭС требует от таможенной службы Республики Беларусь развивать свои информационные технологии с учетом необходимости организации информационного взаимодействия с таможенными службами Казахстана, России, Армении, Киргизии, с Секретариатом Комиссии Таможенного союза.

С учетом роста транзитных потоков необходимо ускорить модернизацию информационных систем в целях их гармонизации с информационными системами таможенных служб государств – членов Европейского союза. Опыт внедрения электронного декларирования показал, что следует развивать информационные системы также в сторону максимально широкого предоставления электронных услуг участникам международной торговли.

В условиях развития и внедрения информационно-телекоммуникационных технологий во все сферы жизнедеятельности человека, общества и государства решение вопросов обеспечения информационной безопасности государства, государственных органов является одним из приоритетных.

Информационная безопасность таможенных органов есть состояние защищенности национальных интересов государства в информационной сфере деятельности таможенных органов.

Правовой режим информационной безопасности таможенных органов – это установленный нормами права особый порядок юридического (правового) регулирования общественных отношений, складывающихся в сфере обеспечения информационной безопасности таможенных органов, осуществляемый при помощи различных юридических средств, направленный на создание состояния защищенности интересов участников информационно-таможенных правоотношений. Правовому режиму информационной безопасности таможенных органов присущ императивный метод правового регулирования. Он предполагает использование властных предписаний абсолютно определенного характера, которые исходят от компетентного вышестоящего государственного органа или должностного лица и обеспечиваются мерами принудительного характера.

Содержание национальных интересов государства раскрывается в Концепции информационной безопасности таможенных органов Республики Беларусь, утвержденной решением Коллегии Государственного таможенного комитета Республики Беларусь от 22 декабря 2006 года. В соответствии с ней выделяют четыре составляющих национальных интересов в информационной сфере деятельности таможенных органов:

– соблюдение конституционных прав и свобод человека и гражданина в области получения и использования таможенной информации, а также информации о сведениях и доказательствах, полученных в ходе оперативно-розыскной деятельности, уголовного и административного судопроизводства;

– информационное обеспечение государственной политики, связанное с доведением до белорусской и международной общественности достоверной информации о государственной политике с обеспечением доступа граждан к открытым государственным информационным ресурсам в таможенной сфере;

– содействие развитию современных информационных технологий отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой

продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– защита информационных ресурсов таможенных органов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых в интересах таможенных органов.

Целью обеспечения информационной безопасности таможенных органов является защита национальных интересов государства в информационной сфере при осуществлении таможенными органами функций по выработке государственной политики и нормативного правового регулирования, контроля и надзора в области таможенного дела, а также функций агента валютного контроля и специальных функций по борьбе с контрабандой, иными преступлениями и административными правонарушениями.

При помощи определенных мер защиты поддерживается и обеспечивается защищенность национальных интересов, под которыми следует понимать управленческие меры, направленные на обеспечение информационной безопасности: административные руководящие документы (приказы, распоряжения и инструкции); аппаратные устройства или дополнительные программы, основной целью которых является предотвращение преступлений и злоупотреблений.

Объекты обеспечения информационной безопасности сгруппированы по сферам жизнедеятельности общества и государства. Выделяется шесть сфер:

1. *Сфера внешней политики*. В ней объектами обеспечения информационной безопасности таможенных органов являются информационные ресурсы представительств таможенной службы Республики Беларусь за рубежом. Через них организовывается трансграничный обмен информацией.

2. *Сфера внутренней политики*. В данной сфере объектами обеспечения выступают: конституционные права и свободы человека и гражданина, являющегося должностным лицом или работником таможенных органов; персональные данные физических лиц; открытые информационные ресурсы таможенных органов.

3. *Сфера экономики*. В ней объектами обеспечения информационной безопасности таможенных органов являются: любая информация, полученная таможенными органами в соответствии с тамо-

женным законодательством Таможенного союза, иными правовыми актами Республики Беларусь и (или) составляющая государственную, коммерческую, банковскую, налоговую или иную охраняемую законом тайну и другую конфиденциальную информацию; документы и сведения, используемые для статистических целей; права правообладателей на объекты интеллектуальной собственности при совершении таможенных операций.

4. *Правоохранительная и судебная сфера*. В них объектами обеспечения выступают информационные ресурсы подразделений, реализующих правоохранительные функции, содержащие специальные сведения и оперативные данные служебного характера.

5. *Сфера общегосударственных информационных и телекоммуникационных систем*. Объектами обеспечения информационной безопасности таможенных органов являются: объекты информатизации таможенных органов, предназначенные для обработки сведений, отнесенных к государственной тайне; технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа; помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

6. *Область науки и техники*, где объектами безопасности выступают: результаты проведенных по заказу таможенных органов фундаментальных, поисковых и прикладных научных исследований, потенциально важных для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Республики Беларусь; открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование, разработанные или полученные в интересах таможенных органов; научно-технические кадры таможенных органов.

Угрозами безопасности информационных и телекоммуникационных средств и систем таможенных органов могут являться:

– нарушения технологии обработки информации ограниченного доступа, обрабатываемой в таможенных органах;

– нарушение законных ограничений на распространение информации ограниченного доступа, обрабатываемой в таможенных органах;

– противоправные сбор и использование информации ограниченного доступа, обрабатываемой в таможенных органах;

– компрометация ключей и средств криптографической защиты информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации или ее подмена;

– несанкционированный доступ к информации, находящейся в базах данных таможенных органов;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– разработка и распространение программ (компьютерных вирусов), нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

– утечка информации по техническим каналам;

– внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения таможенных органов;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии автоматизированных систем таможенных органов.

Сущность обеспечения информационной безопасности таможенных органов отражена в «Основных направлениях развития таможенной службы Республики Беларусь», утвержденных приказом председателя Государственного Таможенного комитета от 08.04.2011 № 125-ОД.

«Обеспечение информационной безопасности – проведение единой политики в области охраны и защиты информационных ресурсов и информации, система мер организационного, технического и иного характера, адекватных угрозам информационным ресурсам таможенных органов, техническим и программным средствам информационных технологий и, как следствие, интересам таможенных органов в целом.

Задачи:

– предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы;

– сохранение полноты, точности, целостности документированной информации, возможности управления процессом обработки и пользования в соответствии с условиями, установленными собственником этой информации или уполномоченным им лицом;

– обеспечение прав физических и юридических лиц на сохранение конфиденциальности документированной информации о них, накапливаемой в информационных системах;

– защита прав субъектов информационных отношений;

– сохранение секретности, конфиденциальности документированной информации в соответствии с правилами, определенными законодательными актами Республики Беларусь.

Целевые индикаторы:

– обеспечение системного, комплексного, своевременного реагирования на возникающие или осуществленные угрозы информационной безопасности таможенных органов;

– создание централизованной, на основе применения современных технических и программных средств защиты информации, системы управления контроля защищенности информационных ресурсов и средств информационных технологий.»

Для решения вышеизложенных задач необходимо обеспечить:

– использование новых автоматизированных информационных технологий в таможенной деятельности и совершенствование действующих программных средств и подсистем, то есть повысить безопасность информационных систем таможенных органов;

– развитие системы управления рисками на основе осуществления таможенных процедур в соответствии с международными стандартами, основанными на последних достижениях в области информационных и управленческих технологий;

– укрепление взаимодействия с зарубежными и международными органами. В связи с этим – определение на общепринятой в Таможенном союзе основе перечня сведений Таможенного союза, которые необходимо относить к конфиденциальным, и возможной их градации; разработка общих технических стандартов в области информационного взаимодействия и информационной безопасности; взаимная возможность использования таможенными органами государств-участников Таможенного союза национальных секретных технологий и средств, обеспечивающих защиту информации; организация допуска сотрудников таможенных органов государств-участников к общим конфиденциальным сведениям, в том числе к национальной государственной тайне, определение общих подходов к ответственности за нарушение конфиденциальности информации; определение порядка возложения ответственности таможенных органов Таможенного союза перед участниками внешнеэкономической деятельности за сохранность конфиденциальности представляемых ими сведений;

– определение порядка проведения контроля выполнения и эффективности принятых мер по защите информации;

– создание специализированного органа по управлению вопросами обеспечения безопасности информации.

В соответствии с вышеизложенным основными направлениями обеспечения информационной безопасности таможенных органов являются:

– организационно-режимное обеспечение защиты сведений, составляющих государственную тайну, и конфиденциальность служебной информации;

– обеспечение физической защиты объектов и средств информатизации таможенных органов;

– обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче;

– обеспечение защиты информации от несанкционированного доступа в автоматизированных информационных системах и локальных и локальных вычислительных сетях таможенных органов;

– обеспечение конфиденциальности и целостности информации в телекоммуникационных каналах, каналах связи и телефонных линиях связи;

– обеспечение безопасности взаимодействия головного таможенного органа государства с отечественными и зарубежными организациями, министерствами и ведомствами;

– организация, координация и финансирование научно-исследовательских и опытно-конструкторских работ в области обеспечения информационной безопасности таможенных органов;

– совершенствование нормативной базы информационной безопасности таможенных органов.

Таким образом, видно, что информационная безопасность таможенных органов охватывает широкий спектр задач, от решения которых зависит эффективность работы как самих таможенных органов, так и эффективность взаимодействия с ними других организаций и ведомств.

Вопросы для самоконтроля

1. Понятие правового режима информационной безопасности таможенных органов.
2. Цели и объекты обеспечения информационной безопасности жизнедеятельности общества и государства.
3. Угрозы безопасности информационных и телекоммуникационных средств и систем таможенных органов.
4. Основные направления и способы обеспечения информационной безопасности таможенных органов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Основы криптографии : учебное пособие для высших учебных заведений по группе специальностей в области информационной безопасности / А. П. Алферов [и др.]. – Москва: Гелиос АРВ, 2005. – 479 с.

2. Бровка, Г. М. Инновационное развитие и национальная безопасность / Г. М. Бровка. – Минск: РИВШ, 2017. – С. 280.

3. Бровка, Г. М. Информационно-коммуникативные технологии как средство стратегии обеспечения инновационной безопасности и достижения национальных интересов / Г. М. Бровка // Экономическая наука сегодня: сборник научных статей/ выпуск № 4 / БНТУ. – Минск, 2016. – С. 140–150.

4. Бровка, Г. М. Обеспечение национальной безопасности в государствах, формирующих инновационную политику: концептуальные подходы // В журн. «Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Я. Купалы. Серыя 1. Гісторыя і археалогія. Філасофія. Паліталогія». – Том 9, № 1, 2017. – С. 135–142.

5. Бровка, Г. М. Основные направления стратегии обеспечения национальной безопасности в условиях инновационного развития и формирования инновационной экономики / Г. М. Бровка // Проблемы обеспечения национальной и региональной безопасности: правовые и информационные аспекты : материалы международной научно-практической конференции. Минск, 2 ноября 2017 г. – Минск: ИНБ, 2018. – Т.1. С. 86–89.

6. Бровка, Г. М. Инновационная безопасность: отдельные аспекты, методологии, теории, практики / В. А. Сакович, Г. М. Бровка / РИВШ. – Минск: 2016. – 320 с.

7. Бровка, Г. М. Инновационные и информационно-коммуникативные технологии в контексте появления новых рисков и угроз / Г. М. Бровка, В. А. Бенюк, В. В. Скурко // Информационные технологии и право (Правовая информатизация – 2015): материалы V Междунар. науч.-практ. конф., Минск, 28 мая 2015 г. – Минск: Нац. центр правовой информ. Респ. Беларусь, 2015. – С. 66–68.

8. Бровка, Г. М. Национальная безопасность как базисный фактор разработки государственной политики инновационного развития / Г. М. Бровка. Проблемы управления № 2(68) 2018. – Академия управления при Президенте Республики Беларусь, 2018. – С. 122–129.

9. Бровка, Г. М. Энергетическая и инновационная безопасность в системе национальной безопасности государства / Г. М. Бровка // Надежность и безопасность энергетики. – 2015. – № 4(31). – С. 14–19.

10. Бровка, Г. М. Стратегия инновационной безопасности государств ЕАЭС / Г. М. Бровка // «Веснік Брэсцкага ўніверсітэта. Серыя 1. Філасофія. Паліталогія. Сацыялогія». – № 2, 2016. – Выдавецтва БрДУ імя А. С. Пушкіна, 2016. – С. 118–122.

11. Бровка, Г. М. Инновационная экономика и национальная безопасность: система формирования и стратегия обеспечения / Г. М. Бровка. – Кишинев, 2016. – 315 с.

12. Бровка, Г. М. Экономическая безопасность : учебник для студентов вузов / В. Б. Мантусов [и др.]; под. общ. ред. В. Б. Мантусова. – 4-е изд. – Москва: ЮНИТИ-ДАНА, 2018. – 567 с.

13. Ванг, У. Безопасная работа в Internet: эффективный самоучитель / У. Ванг. – Санкт-Петербург: ДиаСофтЮП, 2005. – 397 с.

14. Габдыжамалов, Н. М. Информационная безопасность в рамках интеграционных процессов: политологический анализ : автореферат дис. … канд. полит. наук : 23.00.02 / Н. М. Габдыжамалов. – Астана, 2010. – 40 с.

15. Гражданский кодекс Республики Беларусь [Электронный ресурс] : 7 декабря 1998 г., № 218-З : принят Палатой представителей 28 октября 1998 г. : одоб. Советом Респ. 19 ноября 1998 г.: в ред. Закона Респ. Беларусь от 09.01.2017 г. № 14-З // Национальный правовой интернет-портал РБ. – Режим доступа: http://www.pravo.by. – Дата доступа: 10.05.2018.

16. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Российская газета. – Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. – Дата доступа: 23.09.2017.

17. Защита информационного пространства Республики Беларусь: национальная безопасность VS права человека [Электронный ресурс] // Белорусский документационный центр. – Режим доступа: https://bydc.info – Дата доступа: 11.11.2017.

18. Кибербезопасность Беларуси: лучше Литвы, но хуже России [Электронный ресурс] // Sputnik Беларусь. – Режим доступа: https://sputnik.by/defense_safety/20170619/1029367557/kiberbezopasnost-belarusi-luchshe-litvy-no-huzhe-rossii.html. – Дата доступа: 23.09.2017.

19. Кибервойна и кибервойны: как государства противостоят информационным угрозам? [Электронный ресурс] // EurAsia Daily. – Режим доступа: https://eadaily.com/ru/news/2015/11/30/ kibervoyna-i-kibervoiny-kak-gosudarstva-protivostoyat-informacionnym-ugrozam. – Дата доступа: 23.09.2017.

20. Кибервойны (Cyberwarfare) [Электронный ресурс] // АМ Медиа. – Режим доступа: https://www.anti-malware.ru/threats/ cyberwarfare. – Дата доступа: 22.09.2017.

21. Ковалькова, И. А. Защита информационных систем в таможенных органах Республики Беларусь / И. А. Ковалькова // Информационные технологии в технических, правовых, политических и социально-экономических системах : материалы Международной научно-практической конференции, Минск, 20 апр. 2017 г. / редкол.: В. В. Цепкало [и др.]. – Минск: РИВШ, 2017. – 446 с.

22. Ковалькова, И. А. Информационная безопасность в сетях ЭВМ / И. А. Ковалькова // Наука – образованию, производству, экономике : материалы 12-й Международной научно-технической конференции. Т. 4. – Минск: БНТУ, 2014. – С. 178.

23. Ковалькова, И. А. Информационная безопасность таможенных служб / И. А. Ковалькова // Учебно-методический комплекс по учебной дисциплине «Информационная безопасность таможенных служб» для специальности 1-96 01 01 «Таможенное дело» (по направлениям). Электронный учебный материал. – Минск: БНТУ, 2013. – 80 с.

24. Ковалькова, И. А. Криптографические методы обеспечения информационной безопасности / И. А. Ковалькова // Наука – образованию, производству, экономике : материалы 10-й Международной научно-технической конференции. Т. 4. – Минск: БНТУ, 2012 – С. 191.

25. Ковалькова, И. А. Основные направления обеспечения информационной безопасности в таможенных органах Республики Беларусь / И. А. Ковалькова // Наука – образованию, производству, экономике : материалы 11-й Международной научно-технической конференции. Т. 4. – Минск: БНТУ, 2013. – С. 187.

26. Ковалькова, И. А. Основные угрозы информационной безопасности в сфере таможенного дела / И. А. Ковалькова // Наука – образованию, производству, экономике : материалы 13-й Международной научно-технической конференции. – Минск: БНТУ, 2015. – Т. 4. – С. 183–184.

27. Ковалькова, И. А. Электронная цифровая подпись и ее роль в таможенной деятельности / И. А. Ковалькова // «Таможенный союз Республики Беларусь, Республики Казахстан и Российской Федерации: современность и перспективы» : сборник докладов II Международной научно-практической конференции (г. Минск, 22–23 сентября 2011 г.) / Государственный институт повышения квалификации и переподготовки кадров таможенных органов Республики Беларусь, Белорусский национальный технический университет, Белорусский государственный университет; сост. В. Н. Ананьева. – Минск: Белтаможсервис, 2012. – 156 с.

28. Кодекс Республики об административных правонарушениях [Электронный ресурс] : 21 апреля 2003 г., № 194-З : принят Палатой представителей 17 декабря 2002 г. : одоб. Советом Респ. 2 апреля 2003 г. : в ред. Закона Респ. Беларусь от 8.01.2018 г. № 95-З // Национальный правовой интернет-портал РБ. – Режим доступа: http://www.pravo.by – Дата доступа: 10.05.2018.

29. Конституция Республики Беларусь : с изм. и доп., принятыми на республиканских референдумах 24 нояб. 1996 г. и 17 окт. 2004 г. – Минск: Нац. центр правовой информ. Респ. Беларусь, 2016. – 62 с.

30. Леонтьев, В. П. Безопасность в сети Интернет. / В. П. Леонтьев. – Москва: ОЛМА Медиа Групп, 2008. – 256 с.

31. О таможенном регулировании в Республике Беларусь [Электронный ресурс]: Закон Респ. Беларусь, 10 января 2014 г., № 129-З. // Национальный правовой интернет-портал Республики Беларусь. – Режим доступа: http://www.pravo.by. – Дата доступа: 05.04.2018.

32. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 9 янв. 2002 г. № 90-З : в ред. от 8 июля 2008 г. № 366-З : с изм. и доп. от 2 мая 2012 г. № 353-З // Национальный правовой интернет-портал РБ. – Режим доступа: http://www.pravo.by. – Дата доступа: 12.11.2017.

33. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 : в ред. Указа Президента Респ. Беларусь от 24.01.2014 г. – Режим доступа: http://kgb.by – Дата доступа: 12.11.2017.

34. Основные направления развития таможенной службы Республики Беларусь // Утверждено Приказом председателя ГТК от 08.04.2011 № 125-ОД.

35. Петров, А. А. Компьютерная безопасность: Криптографические методы защиты / А. А. Петров. – Москва: ДМК, 2000. – 445 с.

36. Расторгуев, С. П. Основы информационной безопасности : учебное пособие по специальностям «Компьютерная безопасность», «Комплексное обеспечение информационной безопасности автоматизированных систем» и «Информационная безопасность телекоммуникационных систем» / С. П. Расторгуев. – Москва: Академия, 2007. – 186 с.

37. Смит, Р. Э. Аутентификация: от паролей до открытых ключей / Р. Э. Смит. – Москва: Вильямс, 2002. – 424 с.

38. События на площади Таньаньмэнь в Пекине весной 1989 года [Электронный ресурс] // РИА Новости. – Режим доступа: https://ria.ru/politics/20090604/173226397.html. – Дата доступа: 23.09.2017.

39. Столичными следователями устанавливаются обстоятельства коммерческого шпионажа в сфере таможенного представительства [Электронный ресурс] // Следственный комитет Республики Беларусь. – Режим доступа: https://sk.gov.by/ru/news-ru/view/usk-po-g-minsku-ustanavlivajutsja-obstojatelstva-kommercheskogo-shpionazha-v-sfere-tamozhennogo-6359/ – Дата доступа: 08.05.2018.

40. Столлингс, В. Основы защиты сетей: Приложения и стандарты / В. Столлингс. – Москва: Вильямс, 2002. – 429 с.

41. Таможенный Кодекс Евразийского экономического союза [Электронный ресурс] : приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза // КонсультантПлюс. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_215315/. – Дата доступа: 07.04.2018.

42. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одоб. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 18.04.2017 г. № 53-З // Национальный правовой интернет-портал РБ. – Режим доступа: http://www.pravo.by. – Дата доступа: 10.05.2018.

43. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учебное пособие для студентов высших учебных заведений / П. Б. Хорев. – 3-е изд., стер. – Москва: Издательский центр «Академия», 2007. – 256 с.

44. Что такое кибервойна и чем она грозит [Электронный ресурс] // Независимая Уральская газета. – Режим доступа: http://proural.info/society/10148/. – Дата доступа: 22.09.2017.

45. Шавель, А. Н. К вопросу об информационной безопасности в таможенных органах Республики Беларусь / А. Н. Шавель // Наука – образованию, производству, экономике : материалы 14-й Международной научно-технической конференции. – Минск: БНТУ, 2016. – Т. 4. – С. 187.

46. Шавель, А. Н. Современные проблемы информационной безопасности / А. Н. Шавель // Наука – образованию, производству, экономике : материалы 11-й Международной научно-технической конференции. – Т. 4. – Минск: БНТУ, 2013. – С. 179.

47. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2009. – 416 с.

48. Щербаков А. Ю. Современная компьютерная безопасность: теоретические основы, практические аспекты : учебное пособие / А. Ю. Щербаков. – Москва: Книжный мир, 2009. – 351 с.

49. Ярочкин, В. И. Информационная безопасность : учебник для вузов: по гуманитарным и социально-экономическим специальностям / В. И. Ярочкин. – Москва: Трикста: Академический проект, 2005. – 542 с.

Учебное издание

БРОВКА Геннадий Михайлович
КОВАЛЬКОВА Инна Александровна
ШАВЕЛЬ Александр Николаевич

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТАМОЖЕННЫХ ОРГАНАХ

Учебно-методическое пособие для студентов
специальности 1-96 01 01 «Таможенное дело»

Редактор *Ю. В. Ходочинская*
Компьютерная верстка *Е. А. Беспанской*

Подписано в печать 15.01.2019. Формат 60×84 $^{1}/_{16}$. Бумага офсетная. Ризография.
Усл. печ. л. 6,92. Уч.-изд. л. 5,41. Тираж 100. Заказ 652.

Издатель и полиграфическое исполнение: Белорусский национальный технический университет.
Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий № 1/173 от 12.02.2014. Пр. Независимости, 65. 220013, г. Минск.